

Oracle® Integrated Lights Out Manager (ILOM) 3.0

Web Interface Procedures Guide



Copyright © 2008, 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Copyright © 2008, 2010, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.



Contents

Using This Documentation	xiii
1. Web Interface Overview	1
About the Web Interface	2
Browser and Software Requirements	2
Network Addresses Accepted by ILOM	3
Entering an IPv6 Address into a URL or Directory Path	4
CMM and Server SP Web Interface Connection	4
Server SP Web Interface Components	5
CMM ILOM Web Interface	6
Navigation Tabs	9
Navigation Using Jump Links	13
User Management --> Active Directory	14
2. Logging In to and Out of ILOM	15
Before Your Initial Login	16
Logging In to ILOM	16
▼ Log In to ILOM Using the root User Account	17
▼ Set Up a User Account	18
▼ Log In to ILOM as a User	18

Logging Out of ILOM 19

- ▼ Log Out of ILOM 19

Configuring Banner Messages 19

Before You Begin 19

- ▼ Configure Banner Messages in ILOM 20

What Next 20

3. Configuring ILOM Communication Settings 21

Configuring Network Settings 23

Before You Begin 23

- ▼ View and Configure IPv4 Network Settings 25
- ▼ View and Configure Dual-Stack IPv4 and IPv6 Network Settings 27
- ▼ Test IPv4 or IPv6 Network Configuration 31
- ▼ Assign Host Name and System Identifier 31
- ▼ View and Configure DNS Settings 32
- ▼ View and Configure Baud Rate for Serial Port 33
- ▼ Configure x86 Host Serial Port Sharing (Port Owner) 34
- ▼ Enable HTTP or HTTPS Web Access 35
- ▼ Upload the SSL Certificate 37

Configuring Secure Shell Settings 37

Before You Begin 37

- ▼ Enable or Disable SSH 38
- ▼ Generate a New SSH Key 38
- ▼ Restart the SSH Server 38

Configuring the Local Interconnect Interface 39

Before You Begin 39

- ▼ Configure the Local Interconnect Interface 40

4. Managing User Accounts 43

Configuring User Accounts 44

Before You Begin 44

- ▼ Configure Single Sign On 45
- ▼ Set the Session Time-Out 45
- ▼ Add User Accounts and Assign Roles 45
- ▼ Configure a User Account 47
- ▼ Delete a User Account 48
- ▼ View User Sessions 48

Configuring SSH Keys 49

Before You Begin 49

- ▼ Add an SSH Key 49
- ▼ Delete an SSH Key 51

Configuring Active Directory 52

Before You Begin 52

- ▼ View and Configure Active Directory Settings 53
- ▼ Configure Active Directory Tables 57
- ▼ Troubleshoot Active Directory Authentication and Authorization 60

Configuring Lightweight Directory Access Protocol 62

Before You Begin 62

- ▼ Configure the LDAP Server 62
- ▼ Configure ILOM for LDAP 63

Configuring LDAP/SSL Settings 64

Before You Begin 64

- ▼ View and Configure LDAP/SSL Settings 64
- ▼ Configure LDAP/SSL Tables 68
- ▼ Troubleshoot LDAP/SSL Authentication and Authorization 71

Configuring RADIUS 73

Before You Begin	73
▼ Configure RADIUS Settings	73
5. Managing System Components	75
Viewing Component Information and Managing System Components	76
Before You Begin	76
▼ View and Change Component Information	76
▼ Prepare to Remove a Component	78
▼ Return a Component to Service	78
▼ Enable and Disable Components	78
6. Monitoring System Components	79
Monitoring System Sensors, Indicators, and ILOM Event Logs	80
▼ View Sensor Readings	80
▼ Configure System Indicators	81
▼ Configure Clock Settings	82
▼ Configure Timezone Settings	83
▼ Filter Event Log Output	83
▼ View and Clear the ILOM Event Log	85
▼ Configure Remote Syslog Receiver IP Addresses	86
▼ View and Clear Faults	87
7. Monitoring Storage Components and Zone Manager	89
Viewing and Monitoring Storage Components	90
Before You Begin	90
▼ View and Monitor RAID Controller Details	91
▼ View and Monitor Details for Disks That Are Attached to RAID Controllers	92
▼ View and Monitor RAID Controller Volume Details	94
Enabling or Disabling Zone Manager	95

8. Managing System Alerts	97
Managing Alert Rule Configurations	98
Before You Begin	98
▼ Create or Edit Alert Rules	99
▼ Disable an Alert Rule	100
▼ Generate Test Alerts	100
▼ Send Test Email Alert to Specific Alert Destination	101
Configuring SMTP Client for Email Notification Alerts	101
Before You Begin	101
▼ Enable SMTP Client	102
Downloading SNMP MIBs Directly From ILOM	102
Before You Begin	102
▼ Download SNMP MIBs	103
9. Power Monitoring and Management of Hardware Interfaces	105
Summary of Power Management Feature Updates	106
Monitoring System Power Consumption	109
Before You Begin	109
▼ Monitor System Power Consumption	110
▼ Monitor Individual Power Supply Consumption	111
▼ Monitor Power Statistics and Power History	111
Configuring Power Policy Settings to Manage Server Power Usage	113
Before You Begin	113
▼ Configure Power Consumption Policy	114
▼ Configure Server Power Policy Ffor Power Capping	115
Configuring Power Consumption Threshold Notifications	117
Before You Begin	117
▼ View and Configure Notification Thresholds Using the Web Interface	117

Monitoring and Configuring Component Power Allocation Distributions	118
Before You Begin	118
▼ View Server Component Power Allocations	119
▼ Configure Server Power Limit Properties as of ILOM 3.0.8	120
▼ View CMM Component Power Allocations	121
▼ Configure Permitted Power for Blade Slots in CMM as of ILOM 3.0.6	124
▼ Configure Grant Limit for Blade Slots in CMM as of ILOM 3.0.10	125
Configuring Server Power Limit Properties	126
Before You Begin	127
▼ Configure Server Power Limit Properties	127
Monitoring or Configuring CMM Power Supply Redundancy Properties	130
Before You Begin	130
▼ View or Configure CMM Power Supply Redundancy Properties	130
10. Backing Up and Restoring ILOM Configuration	133
Backing Up the ILOM Configuration	134
Before You Begin	134
▼ Back Up the ILOM Configuration	134
Restoring the ILOM Configuration	136
Before You Begin	136
▼ Restore the ILOM Configuration	137
▼ Edit the Backup XML File	139
Resetting the ILOM Configuration	142
Before You Begin	142
▼ Reset the ILOM Configuration to Defaults	142
11. Updating ILOM Firmware	145
Updating the Firmware	146
Before You Begin	146

- ▼ Identify ILOM Firmware Version 147
- ▼ Download New ILOM Firmware Image 147
- ▼ Update the Firmware Image 148
- ▼ Recover From a Network Failure During Firmware Update 149

Resetting ILOM SP 150

- Before You Begin 150
- ▼ Reset ILOM SP 150

12. **Managing Remote Hosts Redirection and Securing the ILOM Remote Console 151**

Managing Remote Hosts 152

- Before You Begin 153

Performing the Initial Setup Tasks to Enable ILOM Remote Console Video Redirection 154

- ▼ Configure ILOM Remote Control Video Redirection Settings 154
- ▼ Register 32-bit JDK File Type When Using Windows Internet Explorer 156

Launching Redirection Using the Oracle ILOM Remote Console 157

- Before You Begin 157
- ▼ Launch the Oracle ILOM Remote Console 158
- ▼ Start, Stop, or Restart Device Redirection 160
- ▼ Redirect Keyboard Input 160
- ▼ Control Keyboard Modes and Key Send Options 161
- ▼ Redirect Mouse Input 162
- ▼ Redirect Storage Media 162
- ▼ Add a New Server Session 164
- ▼ Exit the Oracle ILOM Remote Console 164

Securing the ILOM Remote Console 165

- Before You Begin 165
- ▼ Edit the ILOM Remote Console Lock Option 165

- 13. Managing Remote Hosts Power States 167**
 - Controlling Power States on Remote Server SP or CMM 168
 - Before You Begin 168
 - ▼ Control Power State of Remote Host Server Using Server SP Web 168
 - ▼ Control Power State of Remote Chassis Using the CMM Web Interface 169
 - Managing Host Control of BIOS Boot Device on x86 Systems 169
 - Before You Begin 170
 - ▼ Configure BIOS Host Boot Device Override 170

- 14. Managing TPM and LDom States on SPARC Servers 173**
 - Controlling the TPM State on SPARC Servers 174
 - Before You Begin 174
 - ▼ Control TPM State on a SPARC Server 174
 - Managing LDom Configurations on SPARC Servers 175
 - Before You Begin 176
 - ▼ View Stored LDom Configurations on SPARC T3 Series Server 176
 - ▼ Configure Host Power to Stored LDom Configurations 177
 - ▼ Specify Host Power to a Stored LDom Configuration 178

- 15. Performing Remote Host System Diagnostics 179**
 - Diagnosing x86 Systems Hardware Issues 180
 - Before You Begin 180
 - ▼ Configure Pc-Check Diagnostics for x86 Systems 180
 - ▼ Generate a NMI 181
 - Diagnosing SPARC Systems Hardware Issues 182
 - Before You Begin 182
 - ▼ Configure Diagnostics Settings for SPARC Systems 182
 - Collecting SP Data to Diagnose System Problems 183
 - Before You Begin 183

▼	Collect SP Data to Diagnose System Problems	184
A.	Diagnosing IPv4 or IPv6 ILOM Connection Issues	187
B.	Manual Host OS Configuration Guidelines for Local Interconnect Interface	189
	Index	193

Using This Documentation

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

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

To fully understand the information that is presented in this guide, use the web interface procedures guide in conjunction with other guides in the ILOM 3.0 Documentation Collection. For a description of the guides that comprise the ILOM 3.0 Documentation Collection, see ["Related Documentation" on page xiii](#).

This preface contains the following topics:

- ["Related Documentation" on page xiii](#)
- ["Documentation, Support, and Training" on page xv](#)
- ["ILOM 3.0 Version Numbers" on page xv](#)
- ["Documentation Comments" on page xvi](#)

Related Documentation

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

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

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

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

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

Documentation, Support, and Training

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

ILOM 3.0 Version Numbers

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

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

For example, ILOM 3.1.2.1.a would designate:

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

Documentation Comments

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

<http://docs.sun.com>.

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

Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide,
part number 820-6411-12.

Web Interface Overview

Topics

Description	Links
Learn about ILOM web interface features and functionality	<ul style="list-style-type: none">• “About the Web Interface” on page 2• “Browser and Software Requirements” on page 2• “Network Addresses Accepted by ILOM” on page 3• “CMM and Server SP Web Interface Connection” on page 4• “Server SP Web Interface Components” on page 5• “CMM ILOM Web Interface” on page 6• “Navigation Tabs” on page 9• “Navigation Using Jump Links” on page 13

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• ILOM Overview	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide</i> (820-6410)
• CLI	• CLI Overview	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide</i> (820-6412)
• SNMP and IPMI hosts	• SNMP Overview • IPMI Overview	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide</i> (820-6413)

The ILOM 3.0 Documentation Collection is available at:

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

This chapter introduces the basic information you need to know before you perform procedures using the ILOM web interface.

About the Web Interface

The ILOM web interface is accessible through a browser and uses a standard interface. The ILOM web interface enables you to monitor and manage local and remote systems. One of the most powerful features of 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 ILOM Remote Console application.

Browser and Software Requirements

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.

ILOM supports the browsers listed in the following table.

TABLE 1-1 Supported Web Browsers

Operating System	Web Browser
Oracle Solaris (9 and 10)	<ul style="list-style-type: none">• Mozilla 1.4 and 1.7• Firefox 1.x and above

TABLE 1-1 Supported Web Browsers (*Continued*)

Operating System	Web Browser
Linux (Red Hat, SuSE, Ubuntu, Oracle)	<ul style="list-style-type: none">• Mozilla 1.x and above• Firefox 1.x and above• Opera 6.x and above
Microsoft Windows (98, 2000, XP, Vista)	<ul style="list-style-type: none">• Internet Explorer 5.5, 6.x, 7.x• Mozilla 1.x and above• Firefox 1.x and above• Opera 6.x and above
Macintosh (OSX v10.1 and above)	<ul style="list-style-type: none">• Internet Explorer 5.2• Mozilla 1.x and above• Firefox 1.x and above• Safari – all

Note – ILOM comes preinstalled on your Sun system and includes the Remote Console application. To run the 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>. See [Chapter 12](#) for a list of web browsers and operating systems supported by the Remote Console application.

Network Addresses Accepted by ILOM

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

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

For additional information about dual-stack network configurations, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410). For help with diagnosing IPv4 and IPv6 connection issues, see [“Diagnosing IPv4 or IPv6 ILOM Connection Issues” on page 187](#).

Entering an IPv6 Address into a URL or Directory Path

When entering an IPv6 address into a URL or directory path, the address must be enclosed within brackets to work correctly.

- To transfer a file, type:

```
load -source tftp://[fec0:a:8:b7:214:rfff:fe01:851d]desktop.pkg
```

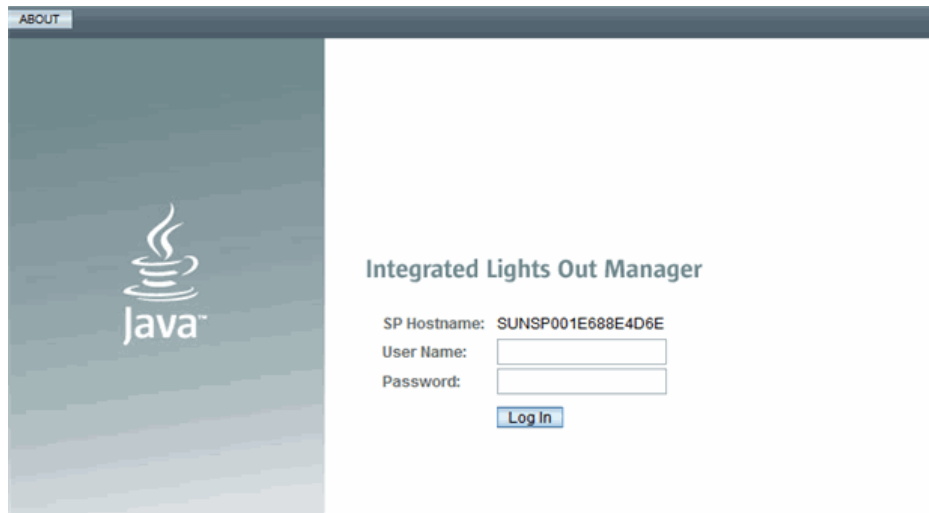
- To enter a URL, type

```
https://[fe80::221:28ff:fe77:1402]
```

For additional information about entering IPv6 addresses, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410). For help with diagnosing IPv4 and IPv6 connection issues, see [“Diagnosing IPv4 or IPv6 ILOM Connection Issues”](#) on page 187.

CMM and Server SP Web Interface Connection

To establish a web interface connection to 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.



ABOUT

Integrated Lights Out Manager

SP Hostname: SUNSP001E688E4D6E

User Name:

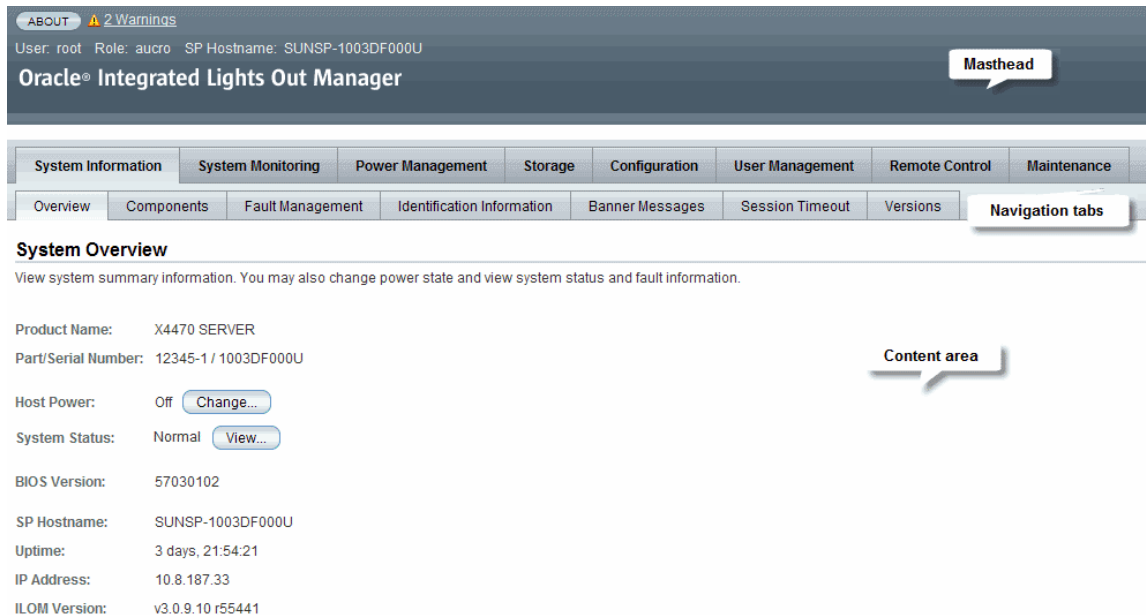
Password:

Server SP Web Interface Components

The main 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 ILOM web interface, see “CMM ILOM Web Interface” on page 6.

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

FIGURE 1-1 ILOM Web Interface Main Page



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 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 may have entered or selected on the page.
- **Log Out button** – Click to end the current session of the web interface.

Note – Use the Refresh and Log Out buttons that are part of the ILOM web interface. Do not use the Refresh or Log Out button on your web browser when you are using the web interface.

The ILOM web interface navigation structure includes tabs and second-level tabs that you can click to open a specific page. When you click the main tab, second-level tabs are displayed, providing you with further options. The content area is where you find information about the specific topic or operation.

CMM ILOM Web Interface

The 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** [Change...](#)
 System Status: [View...](#)
 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 Storage -> Zoning Management features available in ILOM as 3.0.10, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CMM Administration Guide For Sun Blade 6000 and Sun Blade 6048 Modular Systems (820-0052)*

- 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.

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 ILOM Web Interface page, as shown in the previous example.

For more information about the tabs described in this section, see [“Navigation Tabs” on page 9](#).

Navigation Tabs

The following table describes the various tabs and sub-tabs that you can use to access the most common ILOM functions using the web interface. For more detail about how to use the features and functions on the web pages that appear when you select a tab, see the related chapters in this guide.

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

TABLE 1-2 ILOM 3.0 Web Interface Tabs

Main Tab	Second and Third-level Tabs	What You Can Do	Applicable To
System Information			
	Overview	View the product name, part/serial number, host power state, system status state, BIOS version, SP hostname, system uptime, IP address, and ILOM version that is running <ul style="list-style-type: none">• 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 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

TABLE 1-2 ILOM 3.0 Web Interface Tabs (*Continued*)

Main Tab	Second and Third-level Tabs	What You Can Do	Applicable To
	Session Timeout	View the session timeout or change the session timeout parameter	Server SP CMM
	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 ILOM 3.0.10.	Server SP CMM
	Limit	View or configure server power limits. This tab was previously named Budget prior to 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 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			
	RAID --> Controllers	View information for RAID controllers. To get further details, click on a Controller Name	Server SP

TABLE 1-2 ILOM 3.0 Web Interface Tabs (*Continued*)

Main Tab	Second and Third-level Tabs	What You Can Do	Applicable To
	RAID --> Disks	View information for all disks attached to RAID controllers. To view further details, click on a Disk Name	Server SP
	RAID --> Volumes	View information for RAID volumes. To view further details, click on a 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 Timeout 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 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
	Serial Port	View and edit the baud rate of the internal and external serial ports	Server SP CMM

TABLE 1-2 ILOM 3.0 Web Interface Tabs (*Continued*)

Main Tab	Second and Third-level Tabs	What You Can Do	Applicable To
	Clock	View and edit the ILOM clock time manually, or synchronize the 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 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 ILOM, as well as the type of session users have initiated	Server SP CMM
	User Accounts	Add, delete, or modify local ILOM user accounts	Server SP CMM
	LDAP	Configure ILOM access for LDAP users	Server SP CMM
	LDAP/SSL	Configure ILOM access for LDAP users with enhanced security settings enabled by Secure Socket Layer (SSL) technology	Server SP CMM
	RADIUS	Configure ILOM access for RADIUS users	Server SP CMM
	Active Directory	Configure 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
	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

TABLE 1-2 ILOM 3.0 Web Interface Tabs (*Continued*)

Main Tab	Second and Third-level Tabs	What You Can Do	Applicable To
	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 poweron	Server SP
Maintenance			
	Firmware Upgrade	Start the process to obtain an upgrade of the 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 thumbdrive, an external host using CLI, or as a downloaded file	Server SP CMM

Navigation Using Jump Links

As of 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 ILOM web page that includes jump links is shown in the following figure.

User Management --> Active Directory

System Information	System Monitoring	Configuration	User Management	Remote Control	Maintenance
User Accounts	Active Sessions	LDAP	LDAP/SSL	RADIUS	Active Directory

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.

- Settings
- Operator Groups
- Alternate Servers
- Certificate Information
- Custom Groups
- DNS Locator Queries
- Admin Groups
- User Domains

Logging In to and Out of ILOM

Topics

Description	Links
Review the prerequisites	<ul style="list-style-type: none"> • “Before Your Initial Login” on page 16
Log in to ILOM for the first time	<ul style="list-style-type: none"> • “Log In to ILOM Using the root User Account” on page 17
Set up a user account	<ul style="list-style-type: none"> • “Set Up a User Account” on page 18
Log in to ILOM as a regular user	<ul style="list-style-type: none"> • “Log In to ILOM as a User” on page 18
Log out of ILOM	<ul style="list-style-type: none"> • “Log Out of ILOM” on page 19
Configure banner messages in ILOM	<ul style="list-style-type: none"> • “Configure Banner Messages in ILOM” on page 20

Related Topics

For ILOM	Chapter or Section	Guide
<ul style="list-style-type: none"> • Getting Started 	<ul style="list-style-type: none"> • ILOM Getting Started Process • Initial ILOM Setup Procedures Using the Web Interface 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide</i> (820-5523)
<ul style="list-style-type: none"> • CLI 	<ul style="list-style-type: none"> • Logging In to and Out of ILOM 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide</i> (820-6412)

The ILOM 3.0 Documentation Collection is available at:

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

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

Before Your Initial Login

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

- Plan how you want to set up ILOM on your server to work in your data center environment. Refer to the section for establishing communication with ILOM in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- Connect to ILOM over a serial port without a network connection, or log in to ILOM over a network. To log in using a direct serial connection, attach a serial cable to the workstation, terminal, or terminal emulator and to the SER MGT port on the server, or if you are using a modular chassis system, to the chassis monitoring module (CMM) port. To log in using a network connection, attach an Ethernet cable to the NET MGT port on the server or CMM. Refer to your platform documentation for more information.
- Configure the network settings. You can use either DHCP or a static network connection. By default, ILOM will attempt to obtain network settings using DHCP. Refer to the section for connecting to ILOM in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*.
- You must have established initial communication with the ILOM SP (CMM or server).
- You must have created a user account in ILOM.

Logging In to ILOM

Topics

Description	Links	Platform Feature Support
Log in to ILOM and set up a user account	<ul style="list-style-type: none">• "Log In to ILOM Using the root User Account" on page 17• "Set Up a User Account" on page 18• "Log In to ILOM as a User" on page 18	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

▼ Log In to ILOM Using the root User Account

To log in to the ILOM web interface for the first time using the root user account, open a web browser and do the following:

1. Type `http://system_ipaddress` into the web browser.

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

For example:

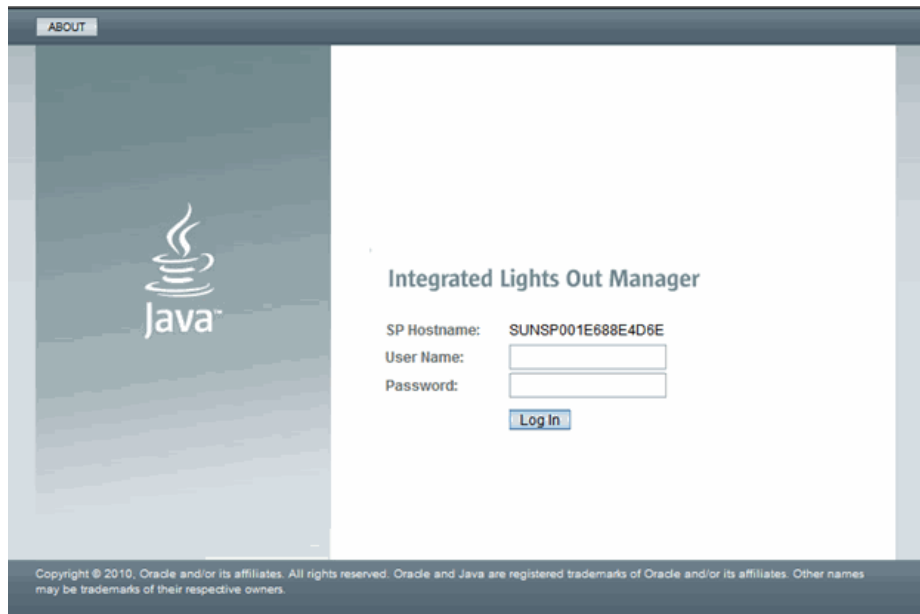
```
http://10.8.183.106
```

or

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

For more information about entering IP addresses in a dual-stack environment, see [“Network Addresses Accepted by ILOM” on page 3](#). For help with diagnosing IPv4 and IPv6 connection issues, see [“Diagnosing IPv4 or IPv6 ILOM Connection Issues” on page 187](#).

The web interface Login page appears.



2. Type the user name and password for the root user account:

User Name: **root**

Password: **changeme**

3. Click Log In.

The Version page in the web interface appears.

▼ Set Up a User Account

Once you are logged in to ILOM, you need to create a regular (non-root) user account. You will use this regular user account to configure ILOM settings for your system and environment.

Follow this step to set up a user account:

● Set up a user account in one of these five classes of users:

- Local users
- Active Directory users
- LDAP users
- LDAP/SSL users
- RADIUS users

You can create and configure with advanced roles up to 10 local user accounts or configure a directory service.

For information about setting up a user account, see ["Add User Accounts and Assign Roles" on page 45](#).

▼ Log In to ILOM as a User

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

Follow these steps to log in to ILOM using a non-root user account:

1. In the web browser, type `http://system_ipaddress`

The web interface Login page appears.

2. Type the user name and password of a user account that you previously configured.

3. Click Log In.

The ILOM web interface appears, displaying the Version page.

Logging Out of ILOM

Topics

Description	Links	Platform Feature Support
Log out of ILOM	<ul style="list-style-type: none">• “Log Out of ILOM” on page 19	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

▼ Log Out of ILOM

- Click the **Log Out** button in the 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 ILOM.

Configuring Banner Messages

Topics

Description	Links	Platform Feature Support
Configure banner messages in ILOM	<ul style="list-style-type: none">• “Configure Banner Messages in ILOM” on page 20	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

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

▼ Configure Banner Messages in ILOM

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. In the 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 logging in to ILOM.	Enter the message in the Login Message text box.

4. In the Login Message Acceptance check box, select the check box to enable the system to display the banner message(s).
5. Click Save.

What Next

After you have set up a user account or configured a directory service, you are now ready to configure ILOM. The remaining chapters in this Oracle ILOM 3.0 Web Interface Procedures Guide provide complete descriptions of the tasks you can perform to access ILOM's functions.

Configuring ILOM Communication Settings

Topics	
Description	Links
Configure network settings	<ul style="list-style-type: none">• “View and Configure IPv4 Network Settings” on page 25• “View and Configure Dual-Stack IPv4 and IPv6 Network Settings” on page 27• “Test IPv4 or IPv6 Network Configuration” on page 31• “Assign Host Name and System Identifier” on page 31• “View and Configure DNS Settings” on page 32• “View and Configure Baud Rate for Serial Port” on page 33• “Enable HTTP or HTTPS Web Access” on page 35• “Upload the SSL Certificate” on page 37• “Configure x86 Host Serial Port Sharing (Port Owner)” on page 34
Configure Secure Shell settings	<ul style="list-style-type: none">• “Enable or Disable SSH” on page 38• “Generate a New SSH Key” on page 38• “Restart the SSH Server” on page 38
Configure the Local Interconnect Interface	<ul style="list-style-type: none">• “Configure the Local Interconnect Interface” on page 40

Related Topics

For ILOM	Chapter or Section	Guide
<ul style="list-style-type: none">• Concepts	<ul style="list-style-type: none">• ILOM Network Configurations	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none">• Getting started	<ul style="list-style-type: none">• Getting Started With ILOM	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide (820-5523)</i>
<ul style="list-style-type: none">• CLI	<ul style="list-style-type: none">• Configuring ILOM Communication Settings	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>
<ul style="list-style-type: none">• IPMI and SNMP hosts	<ul style="list-style-type: none">• Configuring ILOM Communication Settings	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide (820-6413)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Configuring Network Settings

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• “Before You Begin” on page 23	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP
Configure network settings	<ul style="list-style-type: none">• “View and Configure IPv4 Network Settings” on page 25• “View and Configure Dual-Stack IPv4 and IPv6 Network Settings” on page 27• “Test IPv4 or IPv6 Network Configuration” on page 31• “Assign Host Name and System Identifier” on page 31• “View and Configure DNS Settings” on page 32• “View and Configure Baud Rate for Serial Port” on page 33• “Enable HTTP or HTTPS Web Access” on page 35• “Upload the SSL Certificate” on page 37• “Configure x86 Host Serial Port Sharing (Port Owner)” on page 34	<ul style="list-style-type: none">• CMM• x86 system server SP

Before You Begin

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

Network Environment	Before You Begin
IPv4 Network Settings	<ul style="list-style-type: none">• To view network settings, you need the Read Only (o) role enabled. To configure network settings, you need the Admin (a) role enabled.

Network Environment	Before You Begin
Dual-stack IPv4 and IPv6 Network Settings	<ul style="list-style-type: none"> • Prior to configuring ILOM communication settings, ensure that the same IP address is always assigned to ILOM by either assigning a static IP address to ILOM after initial setup, or by configuring your DHCP server to always assign the same IP address to ILOM. This enables ILOM to be easily located on the network. By default, ILOM will attempt to obtain network settings using DHCP. • To view the network settings in ILOM , you need the Read Only (o) role enabled. To configure or test network settings, you need the Admin (a) role enabled. • Verify that your server or CMM has ILOM firmware 3.0.12 or later installed. <p>Note - The dual-stack IPv4 and IPv6 settings cannot be edited at the CMM level in the ILOM web interface. To edit the dual-stack IPv4 and IPv6 properties at the CMM level, you must use the ILOM CLI. For details, see the <i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guides</i>.</p> <ul style="list-style-type: none"> • Verify that support for the IPv6 configuration options in either your platform ILOM Supplement guide or platform Administration guide. • Review the IPv6 enhancements identified in Chapter 2 of the <i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide</i> (820-6410). • ILOM supports a dual-mode TCP/IP stack and is shipped from the factory with both the IPv4 and IPv6 states enabled by default. If necessary, you can optionally disable the IPv6 network state. However, the IPv4 network state must always be enabled in order for ILOM to operate in an IPv4 network environment or in a dual-stack IPv4 and IPv6 network environment. • ILOM supports static and DHCP network settings for both IPv4 and IPv6 network environments. • For IPv6 Stateless auto-configurations, ILOM (3.0.12 or later) requires a network router to be configured for IPv6.

Network Environment	Before You Begin
Dual-stack IPv4 and IPv6	<ul style="list-style-type: none"> • For DHCPv6 auto-configuration options, ILOM (3.0.14 or later) requires a network DHCPv6 server to provide the IPv6 address(es) and DNS information for the device. <p>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</p> <ul style="list-style-type: none"> • 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. <p>You can manually configure the settings for the DNS Name Server in ILOM under the Network DNS target. For instructions on specifying DNS information, see "View and Configure DNS Settings" on page 32.</p>

▼ View and Configure IPv4 Network Settings

Note – This procedure provides instructions for configuring ILOM to operate in an IPv4-only network environment, as is supported in ILOM 3.0.10 and earlier versions of ILOM. If you are configuring ILOM to operate in a dual-stack IPv4 and IPv6 network environment, see ["View and Configure Dual-Stack IPv4 and IPv6 Network Settings" on page 27](#).

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

2. Select Configuration --> Network.

The Network Settings page appears. From the Network Settings page, you can view MAC addresses and configure network addresses for the server's chassis monitoring module (CMM) and service processors (SP).

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 Address.

State: Enabled

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

IP Discovery Mode: DHCP Static

IP Address:

Netmask:

Gateway:

- 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 radio button next to Static 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 ILOM session.

You are prompted to close your web browser.

5. Log back in to 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

Note – This procedure provides instructions for configuring ILOM to operate in a dual-stack IPv4 and IPv6 network environment. If you are configuring ILOM to operate in an IPv4-only network environment, as is supported in ILOM 3.0.10 and earlier versions of ILOM, see [“View and Configure IPv4 Network Settings” on page 25](#).

1. Log in to the ILOM SP web interface or the CMM ILOM 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 ILOM web interface. To edit the dual-stack IPv4 and IPv6 properties at the CMM level, you must use the ILOM CLI. For details, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guides*.

The following illustration shows the 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, Netmask, a 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:fece:5f7e/64
 Static IP Address: ::f128
 Gateway: fe80::211:5dff:febe:5000/128

Dynamic Addresses	
Number	IP Address
1	fec0:a8:b7:214:4fff:fece:5f7e/64

Save

3. Verify that the network State is enabled.

Note – The setting for network State 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 ILOM to operate in an IPv4 network environment or within a dual-stack IPv4 and IPv6 network environment.

4. Perform the network configuration instructions below that apply to your network environment.

- To manually configure a static IP, see the steps below for IPv4 and/or see the steps for IPv6.
 - Steps to manually configure a static IPv4 address:

Steps	Description
a.	Enable the radio button for Static IP.
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.

- Steps to manually configure a static IPv6 address:

Step	Description
•	Type the IP address for the device in the IP 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 ILOM, as well as enable one or more of the IPv6 auto-configuration options in ILOM if desired.

- **To enable DHCP to automatically assign an IPv4 address**, select the IPv4 DHCP radio button.
- **To enable one or more of the IPv6 auto-configuration options**, select the appropriate option(s) described below.
 - Set IPv6 auto-configuration options.

IPv6 Auto-Configuration Option	Description
Stateless (enabled by default)	When enabled, the Stateless auto-configuration option is run to learn the IPv6 Stateless address(es) 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 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 ILOM as of 3.0.14.

Note – As of 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, 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.

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

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

Note – Changing the static IP address on the device (SP or CMM) will end all active ILOM sessions to the device. A message will appear prompting you to close your browser session. You will need to log back in to 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 ILOM sessions to the device. You can verify the newly learned auto-configured addresses on the Network tab.

6. To test the IPv4 or IPv6 network configuration from ILOM, use the Network Test Tools (Ping or Ping6). For details, see ["Test IPv4 or IPv6 Network Configuration"](#) on page 31.

▼ Test IPv4 or IPv6 Network Configuration

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

Tools

The Test Tools dialog appears.

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

Field	Description
Test Type	<ul style="list-style-type: none">• Select Ping to test the IPv4 network configuration. or <ul style="list-style-type: none">• 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).

▼ Assign Host Name and System Identifier

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select 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

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

2. Select Configuration --> DNS.

The DNS Configuration page appears.

3. You can have DHCP assign DNS Name Server and Search Path automatically, or you can choose to assign the addresses manually.

- To automatically assign the addresses, click the radio button 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.

System Information	System Monitoring	Power Management	Configuration	User Management	Remote Control	Maintenance		
System Management Access	Alert Management	Network	DNS	Serial Port	Clock	Timezone	Syslog	SMTP Client

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

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


The Serial Port Settings page appears. See the following figure.

System Information	System Monitoring	Power Management	Configuration	User Management	Remote Control	Maintenance		
System Management Access	Alert Management	Network	DNS	Serial Port	Clock	Timezone	Syslog	SMTP Client

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 settings must 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 take effect on 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 no access to the serial port. All serial port settings will be that of the Host Server.

Owner:

Host Serial Port

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

Baud Rate:

Flow Control:

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

4. Select the baud rate for the internal serial port from the Host Serial Port Baud Rate drop-down list.

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

5. Select the baud rate for the external serial port from the External Serial Port Baud Rate drop-down list.

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 Sharing (Port Owner)

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



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

1. Log in to the ILOM SP 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 serial port sharing setting by default is Service Processor.

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 effect in ILOM.

5. Use a dongle cable to connect the serial host to the server.

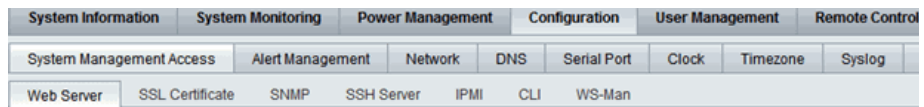
For details on how to use a dongle cable to attach devices to the server, see the platform documentation supplied with your server.

▼ Enable HTTP or HTTPS Web Access

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

2. Select 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 must log into the CLI and enable HTTP or HTTPS access.

HTTP Webservice:

HTTP Port:
The default is: 80

HTTPS Webservice: Enabled

HTTPS Port:
The default is: 443

3. Select the HTTP or HTTPS web server.

- **To enable HTTP** – Select Enabled from the drop-down list. You can also select:
 - Redirect HTTP Connection to HTTPS – HTTP connections are automatically redirected to HTTPS.

- Disabled – Turn HTTP off.
 - **To enable HTTPS** – Select the HTTPS Web Server Enabled check box.
- 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 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 Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

4. Assign an HTTP or HTTPS port number.
5. Click Save for your settings to take effect.
6. To edit IP addresses assigned to the SP interfaces, do the following:
 - a. Select Configuration --> Network to access the Network Settings page.
 - b. Select the radio button for Use the Following IP Address.
 - c. Enter values for IP Address, Subnet Mask, and Gateway in the text boxes.
 - d. Click Save for your new settings to take effect.

After assigning (or changing) an IP address, the connection made to ILOM using the former IP address will timeout. Use the newly assigned IP address to connect to ILOM.

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

State: Enabled

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

IP Discovery Mode: DHCP Static

IP Address:

Netmask:

Gateway:

▼ Upload the SSL Certificate

Note – 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.

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Select 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. **Once you have uploaded the certificate and private key, click the OK button to reset the ILOM web server and begin using the new SSL certificate.**
The ILOM web server must be reset for the new certificate to take effect.

Configuring Secure Shell Settings

Topics

Description	Links	Platform Feature Support
Configure Secure Shell settings	<ul style="list-style-type: none">• "Enable or Disable SSH" on page 38• "Generate a New SSH Key" on page 38• "Restart the SSH Server" on page 38	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

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

▼ Enable or Disable SSH

Note – SSH is enabled by default in ILOM.

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

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

Follow these steps to restart the SSH server:

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

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• “Before You Begin” on page 39	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP
Configure the Local Interconnect Interface	<ul style="list-style-type: none">• “Configure the Local Interconnect Interface” on page 40	

Before You Begin

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

- Review the concepts describing the use of a Local Interconnect Interface between the ILOM SP and the host OS. For details, see *“Local Interconnect Interface: Local Connection To ILOM From Host Operating System”* in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410).
- Review the ILOM descriptions for the Local Host Interconnect configuration settings. For details, see *“Local Host Interconnect Configuration Settings in ILOM”* in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410).
- Verify that your server is running ILOM 3.0.12 or a later version of ILOM.
- Verify that your platform supports the Local Interconnect Interface. Refer to your platform server ILOM Supplement guide or Administration guide.

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

- Automatic configuration of the Local Interconnect Interface requires the `Host Managed` (`hostmanaged`) setting in ILOM to be enabled (set to `True`), as well as the installation of the Oracle Hardware Management Pack 2.1.0 or later software on the server. For more information about installing the Oracle Hardware Management Pack 2.1.0 software, see the *Oracle Server Hardware Management Pack User’s Guide* (821-1609).

- Manual configuration of the Local Interconnect Interface between the ILOM SP and the host operating system requires the Host Managed (`hostmanaged`) setting in ILOM to be disabled (set to `False`), as well as other configuration settings to be set on the host operating system.

For guidelines for configuring the host OS connection point on the Local Interconnect Interface, see “[Manual Host OS Configuration Guidelines for Local Interconnect Interface](#)” on page 189.

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

▼ Configure the Local Interconnect Interface

1. **Log in to the ILOM SP 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 to configure the USB Ethernet Parameters appears.

Configure USB Ethernet Parameters

These parameters can be used to control the internal network connection between the Host and the Service Processor. Typically, the *HostManaged* 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 *HostManaged*.

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

Host Managed: True

State: Enabled

IP Address:

Netmask:

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 clicking `True` in the `Host Management` checkbox to enable this setting.

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 ILOM Interconnect. For more information, see the section about configuring the Local ILOM Interconnect in the *Oracle Server Hardware Management Pack User's Guide* (821-1609).

- or -

- Manually assign non-routable IPv4 addresses to each connection point on the Local Interconnect Interface by specifying the following properties in the `Configure USB Ethernet Parameters` dialog:

Field	Instructions and Description
Host Managed	Clear the checkbox for <code>Host Managed</code> to disable the host managed mode.
State	Click the checkbox for <code>State</code> to manually enable the local interconnect mode between the ILOM SP and the host OS. The <code>State</code> is, by default, disabled.
IP Address	ILOM, by default, provides a default non-routable IPv4 address for the ILOM SP connection point on the Local Interconnect Interface. This default IPv4 address (169.254.182.76) should not be changed unless a conflict exists in your network environment with this IPv4 address.
NetMask	ILOM, by default, provides a default IPv4 <code>Netmask</code> address for the ILOM SP connection point on the Local Interconnect Interface. This default IPv4 <code>Netmask</code> (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 ILOM SP and the host OS, the setting for `Host Managed` must be unchecked (disabled). To prevent the use of the Local Interconnect Interface between the ILOM SP and the host OS, both the settings for `Host Managed` and `State` must be unchecked (disabled).

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

Note – If you chose to manually configure the Local Interconnect Interface in 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 189](#).

Managing User Accounts

Topics	
Description	Links
Configure user accounts	<ul style="list-style-type: none">• "Configure Single Sign On" on page 45• "Set the Session Time-Out" on page 45• "Add User Accounts and Assign Roles" on page 45• "Configure a User Account" on page 47• "Delete a User Account" on page 48• "View User Sessions" on page 48
Configure SSH user key	<ul style="list-style-type: none">• "Add an SSH Key" on page 49• "Delete an SSH Key" on page 51
Configure Active Directory settings	<ul style="list-style-type: none">• "View and Configure Active Directory Settings" on page 53• "Configure Active Directory Tables" on page 57• "Troubleshoot Active Directory Authentication and Authorization" on page 60
Configure LDAP settings	<ul style="list-style-type: none">• "Configure the LDAP Server" on page 62• "Configure ILOM for LDAP" on page 63
Configure LDAP/SSL settings	<ul style="list-style-type: none">• "View and Configure LDAP/SSL Settings" on page 64• "Configure LDAP/SSL Tables" on page 68• "Troubleshoot LDAP/SSL Authentication and Authorization" on page 71
Configure RADIUS settings	<ul style="list-style-type: none">• "Configure RADIUS Settings" on page 73

Related Topics

For ILOM	Chapter or Section	Guide
<ul style="list-style-type: none">• Concepts	<ul style="list-style-type: none">• User Account Management• Guidelines for Managing User Accounts	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none">• CLI	<ul style="list-style-type: none">• Managing User Accounts	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>
<ul style="list-style-type: none">• SNMP	<ul style="list-style-type: none">• Managing User Accounts	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide (820-6413)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Configuring User Accounts

Topics

Description	Links	Platform Feature Support
Configure user accounts	<ul style="list-style-type: none">• "Configure Single Sign On" on page 45• "Set the Session Time-Out" on page 45• "Add User Accounts and Assign Roles" on page 45• "Configure a User Account" on page 47• "Delete a User Account" on page 48• "View User Sessions" on page 48	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

- To set properties for Single Sign On and Session Time-Out, you need the Admin (a) role enabled.
- To set properties for User Management (user accounts and roles), you need the User Management (u) role enabled.

▼ Configure Single Sign On

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select **User Management --> User Accounts**.
The User Account Settings page is displayed.
3. Click the check box next to **Enable Single Sign On** to enable the feature, or deselect the check box to disable the feature.

▼ Set the Session Time-Out

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

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select **System Information --> Session Time-Out**.
The Session Time-Out page appears.
3. Select your preferred time increment from the drop-down list.
4. Click the **Apply** button to save your change.

▼ Add User Accounts and Assign Roles

Note – Only accounts with the User Management (u) role are allowed to add, modify, or delete user accounts. However, you need only the Read Only (o) role to modify your own password. If a new user is assigned the User Management (u) role, those privileges are also automatically granted for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to ILOM.

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select **User Management --> User Accounts**.
The User Account Settings page appears.

3. In the Users table, click Add.

The Add User dialog 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: ▾

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. Type a user name in the User Name field.

b. Choose a role. Options include:

- Advanced Role for all new ILOM 3.0 installations. Choosing Advanced Role gives you the option of selecting Admin (a), Console (c), Read Only (o), User Management (u), Reset and Host Control (r), and Service (s). For a description of the roles and privileges assigned to user accounts, see “Roles for ILOM User Accounts” in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- Administrator or Operator for customers who are upgrading from ILOM 2.0 to ILOM 3.0.
- None

c. Select the appropriate roles.

d. Type a password in the Password field.

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.

- e. Retype the password in the Confirm Password field to confirm the password.
- f. When you are done entering the new user's information, click Save.

The User Account Settings page is redisplayed. The new user account and associated information is listed on the User Account Settings page.

▼ Configure a User Account

Note – You can modify a user account by changing the user's password, and the user's network and serial privileges. To add, modify, or delete user accounts you need the User Management (u) role enabled.

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select User Management --> User Accounts.
The User Account Settings page appears.
3. In the Users table, select a radio button next to the user account you want to modify and click Edit.

A dialog 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 chose Administrator or Operator, ILOM will automatically assign the roles. For example, the two following figures identify the roles assigned by ILOM for Administrator and Operator.

Roles: Administrator ▼

<input checked="" type="checkbox"/> Admin (a)	<input checked="" type="checkbox"/> User Management (u)
<input checked="" type="checkbox"/> Console (c)	<input checked="" type="checkbox"/> Reset and Host Control (r)
<input checked="" type="checkbox"/> Read Only (o)	<input type="checkbox"/> Service (s)

Roles: Operator ▼

<input type="checkbox"/> Admin (a)	<input type="checkbox"/> User Management (u)
<input checked="" type="checkbox"/> Console (c)	<input checked="" type="checkbox"/> Reset and Host Control
<input checked="" type="checkbox"/> Read Only (o)	<input type="checkbox"/> Service (s)

5. Type a new password in the New Password field.

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. Retype the password in the Confirm New Password field to confirm the password.
7. After you have modified the account information, click Save for your changes to take effect, or click Close to return to the previous settings.
The User Account Settings page is redisplayed with your changes.

▼ Delete a User Account

Note – To add, modify, or delete user accounts you need the User Management (u) role enabled.

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select User Management --> User Accounts.
The User Account Settings page appears.
3. Select the radio button next to the user account you want to delete.
4. In the Users table, click Delete.
A confirmation dialog opens.
5. Click OK to delete the account or click Cancel to stop the process.
The User Account Settings page refreshes with the user account you deleted no longer listed.

▼ View User Sessions

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select User Management --> Active Sessions.
The Active Sessions page appears. You can find the user name, the date and time that the user initiated the session, the types of session of the users currently logged in to ILOM, and the mode. If you are using ILOM 3.0.4 or a later version of ILOM, you can also view each user's assigned role.

Configuring SSH Keys

Topics

Description	Links	Platform Feature Support
Configure SSH user key	<ul style="list-style-type: none">• "Add an SSH Key" on page 49• "Delete an SSH Key" on page 51	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

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.

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

▼ Add an SSH Key

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Select 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:

Key Upload

Transfer Method:

Select File:

4. Select the user from the User drop-down list.

5. Select a transfer method from the Transfer Method drop-down list.

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:

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.



The image shows a web form titled "Key Upload". It contains the following fields:

- Transfer Method:** A dropdown menu with "SCP" selected.
- Host:** A text input field.
- Filepath:** A text input field.
- Username:** A text input field.
- Password:** A text input field.

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

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

2. Select **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

Topics

Description	Links	Platform Feature Support
Configure Active Directory settings	<ul style="list-style-type: none">• "View and Configure Active Directory Settings" on page 53• "Configure Active Directory Tables" on page 57• "Troubleshoot Active Directory Authentication and Authorization" on page 60	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

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

▼ View and Configure Active Directory Settings

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

2. Select 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:
IP Address or Hostname

Port: Autoselect
The default is: Autoselect (0)

Timeout:

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:

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

Certificate Information

Certificate File Status: certificate present [\(details\)](#)

Certificate File Upload

Transfer Method:

Select File:

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

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 displayed 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 <code>autoselect</code> is selected, the port is set to 0. Available in the unlikely event of a non-standard TCP port being used.
Timeout	4	Timeout 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 ILOM 3.0.4, an expanded search mode is available. If enabled, an expanded search mode is used 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 ILOM 3.0.10, the Strict Credential Error Mode is available. If the mode is set to disabled (clear checkbox), user-credential errors are retried on other servers that are available (either configured via alternate-server table or found by DNS queries). The disabled state allows users from separate, disjoint domains to log in to ILOM as long as that domain authentication server is available. If the mode is set to enabled (checked checkbox), 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 on “details” for information about issuer, subject, serial number, valid_from, valid_to, and version.

6. Complete the “Certificate File Upload” section by selecting a transfer method for uploading the certificate file and the requested parameters.

Note – This section is only required if Strict Certificate Mode is going to be enabled. If Strict Certificate Mode is disabled, data will still be protected but a certificate will not be needed.

The following table describes the required parameters for each transfer method:

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

7. Click the Load Certificate button or Remove Certificate button.

8. If a certificate is loaded, click on 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 Tables

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

The Active Directory page appears.
- 3. At the bottom 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. Select the radio button of the individual table, 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:**

The Admin Groups table contains the names of the Microsoft Active Directory groups in the Distinguished Name (DN) format, Simple Name format, or NT-Style Name.

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 Microsoft Active Directory groups in the Distinguished Name (DN) format, Simple Name format, or NT-Style Name.

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 Microsoft Active Directory groups in the Distinguished Name (DN) format, Simple Name format, or NT-Style Name. The associated roles for the entry are also configured.

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.

In the example below, the domain listed in entry 1 shows the principle format that is used in the first attempt to authenticate the user. Entry 2 shows the complete Distinguished Name, which Active Directory would use if the attempt to authenticate with the first entry failed.

Note – In the example below, <USERNAME> will be replaced with the user’s login name. During authentication, the user’s login name replaces <USERNAME>.

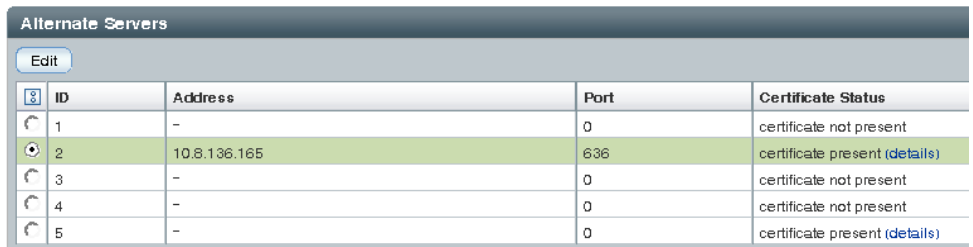
ID	Domain
1	<USERNAME>@sales.east.oracle.com
2	CN=<USERNAME>,CN=Users,DC=sales,DC=east,DC=oracle,DC=com

■ **Alternate Servers Table:**

The Alternate Servers table provides redundancy as well as a choice of different servers if required due to isolated 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:



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:

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 it can be overridden by using the format <PORT:636>. Also, named services specific for the domain being authenticated can be specified by using the <DOMAIN> substitution marker.

Name	Domain
1	_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
2	_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

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

2. Select **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.

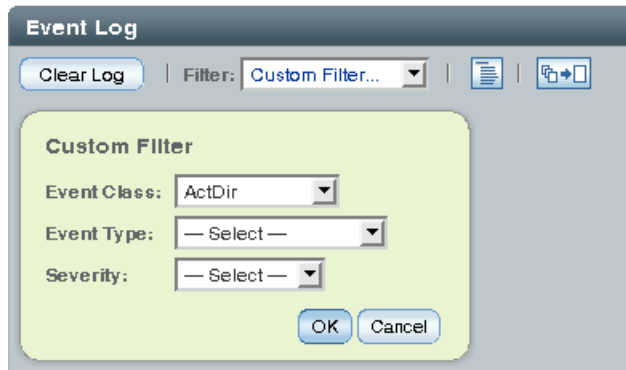
Choices are None, High, Medium, Low, and Trace.

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.



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 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

Topics

Description	Links	Platform Feature Support
Configure LDAP settings	<ul style="list-style-type: none">• "Configure the LDAP Server" on page 62• "Configure ILOM for LDAP" on page 63	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

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

▼ Configure the LDAP Server

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

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

For example:

```
userPassword: {CRYPT}ajCa2He4PJhNo
```

or

```
userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46.
```

2. **Add object classes `posixAccount` and `shadowAccount`, and populate the required property values for this schema (RFC 2307). See the following table for a description of the required property values.**

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

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

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

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

See your LDAP server documentation for more details.

▼ Configure ILOM for LDAP

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

2. Select User Management --> LDAP.

The LDAP Settings page appears.

3. Enter the following values:

- **State** – Select the Enabled check box to authenticate LDAP users.
- **Role** – The default role of LDAP users.
- **Address** – Either the IP address or DNS name of the LDAP server.
- **Port** – The port number on the LDAP server. The default port is 389.
- **Searchbase** – Type the branch of your LDAP server to search for users.
- **Bind DN** – Type the Distinguished Name (DN) of a read-only proxy user on the LDAP server. ILOM must have read-only access to your LDAP server to search for and authenticate users.
- **Bind Password** – 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 ILOM using an LDAP user name and password.

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

Configuring LDAP/SSL Settings

Topics

Description	Links	Platform Feature Support
Configure LDAP/SSL settings	<ul style="list-style-type: none">• "View and Configure LDAP/SSL Settings" on page 64• "Configure LDAP/SSL Tables" on page 68• "Troubleshoot LDAP/SSL Authentication and Authorization" on page 71	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

- To configure LDAP/SSL settings, you need the User Management (u) role enabled.
- To view authentication and authorization events, you need the Read Only (o) role enabled.
- To configure the Optional User Mapping property, you must be using ILOM 3.0.4 or a later version of ILOM.

▼ View and Configure LDAP/SSL Settings

Follow these steps to view and configure LDAP/SSL settings:

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Select 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:

Port: Autoselect

Timeout:

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		
<input type="button" value="Edit"/>		
ID	Name	
1	CN=SuperAdmin,OU=Groups,DC=davide,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 <code>autoselect</code> is enabled, then the port is set to 0. Available in the unlikely event of a non-standard TCP port being used.
Timeout	4	Timeout 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 (Web)	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.
Optional User Mapping	Disabled	Enabled Disabled As of 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	certificate present (details)	Click on “details” for information about issuer, subject, serial number, valid_from, valid_to, and version.

6. Complete the “Certificate File Upload” section by selecting a transfer method for uploading the certificate file.

Note – This section is only required if Strict Certificate Mode is used. If Strict Certificate Mode is disabled, data will still be protected but a certificate will not be needed.

The following table describes the required parameters for each transfer method:

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

7. Click the **Load Certificate** button or **Remove Certificate** button.

8. If a certificate was loaded, click on the “details” link in the web interface 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 LDAP/SSL Tables

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

2. Select 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. Select the radio button of the individual table, 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.

Note – <USERNAME> will be replaced with the user’s login name during authentication. Either the principle or Distinguished Name format is supported.

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:

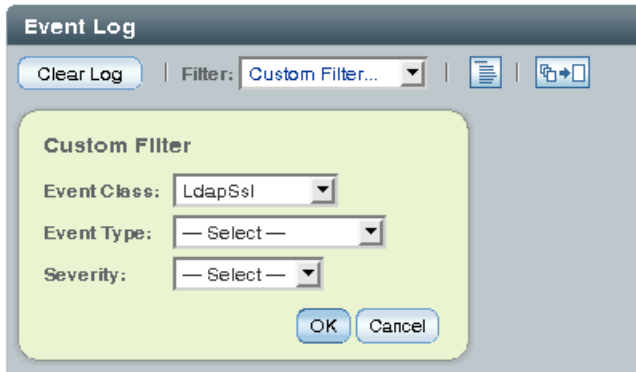
Alternate Servers				
Edit				
ID	address	Port	Certificate Status	
1	-	0	certificate not present	
2	-	0	certificate present details	
3	-	0	certificate not present	
4	-	0	certificate not present	
5	-	0	certificate not present	

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

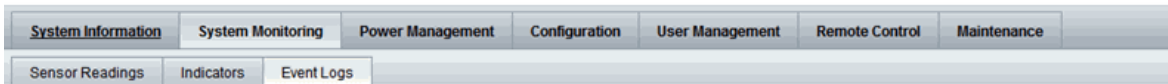
1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select **User Management --> LDAP/SSL**.
The LDAP/SSL page appears.
3. In the **Log Detail** drop-down list, select the level of detail that you would like the event log to capture.
Choices are None, High, Medium, Low, and Trace.
4. Click **Save** to save your changes.
5. Attempt an authentication to generate events:
 - a. Select **System Monitoring --> Event Logs**.
 - b. In the **Filter** drop-down list, select **Custom Filter**.



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					
Clear Log Filter: All Events					
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

Topics

Description	Links	Platform Feature Support
Configure RADIUS settings	<ul style="list-style-type: none">• "Configure RADIUS Settings" on page 73	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

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

▼ Configure RADIUS Settings

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select 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. Enter the IP address of the RADIUS server, and the shared secret your RADIUS server uses to authenticate users.

State: Enabled

Roles: ▼

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

Address:
IP Address or Hostname

Port:
The default is: 1812

Shared Secret:

3. Complete the settings.

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, <code>aucr</code> s, 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 System Components

Topics

Description	Links
Manage system components	<ul style="list-style-type: none">• “Viewing Component Information and Managing System Components” on page 76• “Prepare to Remove a Component” on page 78• “Return a Component to Service” on page 78• “Enable and Disable Components” on page 78

Related Topics

For ILOM	Chapter or Section	Guide
<ul style="list-style-type: none">• Concepts	<ul style="list-style-type: none">• About Fault Management	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none">• CLI	<ul style="list-style-type: none">• Managing System Components	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Viewing Component Information and Managing System Components

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• "Before You Begin" on page 76	<ul style="list-style-type: none">• x86 systems server SP• SPARC system server SP
View and manage system components	<ul style="list-style-type: none">• "View and Change Component Information" on page 76• "Prepare to Remove a Component" on page 78• "Return a Component to Service" on page 78• "Enable and Disable Components" on page 78	<ul style="list-style-type: none">• CMM

Before You Begin

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

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

▼ View and Change Component Information

Follow these steps to view and change component information:

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Select 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 drop-down menu. Components that are in a faulted state cannot be modified. To view further details, click on a Component Name.

Component Status

Filter: All Components

Component Name	Type	Fault Status
/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	-

- 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.

Integrated Lights Out Manager

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

Close

▼ Prepare to Remove a Component

Follow these steps to prepare to remove a component:

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Select System Information --> Components.**
3. The Component Management page appears. **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

Follow these steps to return a component to service:

1. **Log in to the ILOM SP web interface or the CMM ILOM 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 and Disable Components

Follow these steps to enable and disable components:

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

Monitoring System Components

Topics

Description	Links
View sensor readings	<ul style="list-style-type: none"> • “View Sensor Readings” on page 80
Configure system indicators, clock, and timezone settings	<ul style="list-style-type: none"> • “Configure System Indicators” on page 81 • “Configure Clock Settings” on page 82 • “Configure Timezone Settings” on page 83
Filter, view, clear, and configure event logs	<ul style="list-style-type: none"> • “Filter Event Log Output” on page 83 • “View and Clear the ILOM Event Log” on page 85 • “Configure Remote Syslog Receiver IP Addresses” on page 86
View fault status	<ul style="list-style-type: none"> • “View and Clear Faults” on page 87

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• System Monitoring and Alert Management	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
• CLI	• Monitoring System Sensors, Indicators, and ILOM Event Logs	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>
• SNMP	• Monitoring the System	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference (820-6413)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Monitoring System Sensors, Indicators, and ILOM Event Logs

Topics

Description	Links	Platform Feature Support
View sensor readings	<ul style="list-style-type: none">• "View Sensor Readings" on page 80	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP
Change the state of a system indicator	<ul style="list-style-type: none">• "Configure System Indicators" on page 81	<ul style="list-style-type: none">• CMM
View and set clock settings	<ul style="list-style-type: none">• "Configure Clock Settings" on page 82	
Configure timezone settings	<ul style="list-style-type: none">• "Configure Timezone Settings" on page 83	
Set filters for event log data	<ul style="list-style-type: none">• "Filter Event Log Output" on page 83	
View and clear the event log	<ul style="list-style-type: none">• "View and Clear the ILOM Event Log" on page 85	
Set the remote syslog receiver IP addresses	<ul style="list-style-type: none">• "Configure Remote Syslog Receiver IP Addresses" on page 86	
View the fault state of a component	<ul style="list-style-type: none">• "View and Clear Faults" on page 87	<ul style="list-style-type: none">• Most x86 system server SP• Most SPARC system server SP• CMM

▼ View Sensor Readings

Follow these steps to view sensor readings:

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

Before You Begin

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

Follow these steps to configure system indicators:

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select 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, do the following:

- 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 click the Actions drop-down 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

Before You Begin

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

Follow these steps to configure clock settings:

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

2. Select 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 drop-down 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. Select 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.

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

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

▼ Configure Timezone Settings

Before You Begin

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

Follow these steps to configure timezone settings:

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

2. Select Configuration --> Timezone.

The Timezone Settings page appears.

3. Select the timezone using the Timezone drop-down list.

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

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

▼ Filter Event Log Output

Follow these steps to filter event log output:

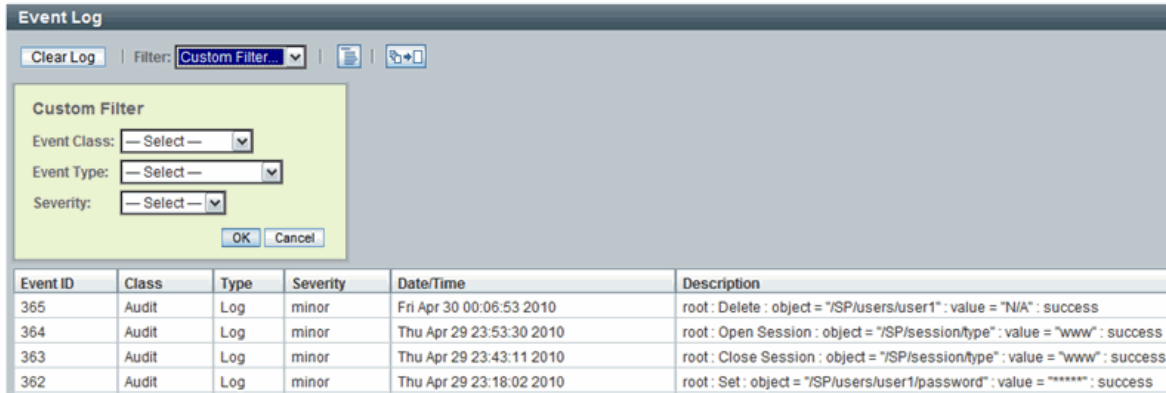
1. Log in to the ILOM SP web interface or the CMM ILOM web interface.

2. Select 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.



3. In the Event Log page, choose from among the following standard filters:

- All Events
- Class: Fault
- Type: Action
- Severity: Down
- Severity: Critical

4. Alternatively, you can choose from among the custom output filters shown in the following figure.

The table below the figure lists the options available in each 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	

Event Class	Event Type	Severity
IPMI	Warning	
Fault		
System		
ActDir		

▼ View and Clear the ILOM Event Log

Before You Begin

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

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

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

2. Select 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	<ul style="list-style-type: none"> • 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 pushed. • 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 ILOM time, the 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 ILOM event log accumulates many types of events, including copies of IPMI entries. Clearing the ILOM event log will clear all entries in the log, including the IPMI entries. However, clearing the ILOM event log entries will not clear the actual entries posted directly to an IPMI log.

▼ Configure Remote Syslog Receiver IP Addresses

Before You Begin

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

Follow these steps to configure remote syslog receiver IP addresses:

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

2. Select Configuration --> Syslog.

The Syslog page appears.

System Information **System Monitoring** **Power Management** **Configuration** **User Management** **Remote Control** **Maintenance**

System Management Access **Alert Management** **Network** **DNS** **Serial Port** **Clock** **Timezone** **Syslog** **SMTP Client**

Syslog

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

Server 1:
IP Address or Hostname

Server 2:
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.

▼ View and Clear Faults

Before You Begin

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

Follow these steps to view or clear faults using the ILOM web interface.

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

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

The Fault Management page appears, listing faulted components by ID, FRU, and TimeStamp.

- 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 on 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 ILOM.

4. To clear the status of faulted components shown in 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, then select Clear Faults.

Monitoring Storage Components and Zone Manager

Topics

Description	Links
View and monitor storage details for HDDs and RAID controllers	<ul style="list-style-type: none">• “View and Monitor RAID Controller Details” on page 91• “View and Monitor Details for Disks That Are Attached to RAID Controllers” on page 92• “View and Monitor RAID Controller Volume Details” on page 94
Enable or disable Zone Manager	<ul style="list-style-type: none">• “Enabling or Disabling Zone Manager” on page 95

Related Topics

For ILOM	Chapter or Section	Guide
<ul style="list-style-type: none">• Concepts	<ul style="list-style-type: none">• Storage Monitoring and Zone Management	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none">• CLI	<ul style="list-style-type: none">• Monitoring Storage Components and Zone Manager	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Viewing and Monitoring Storage Components

Topics

Description	Links	Platform Feature Support
View and monitor storage details for HDDs and RAID controllers	<ul style="list-style-type: none">• “View and Monitor RAID Controller Details” on page 91• “View and Monitor Details for Disks That Are Attached to RAID Controllers” on page 92• “View and Monitor RAID Controller Volume Details” on page 94	<ul style="list-style-type: none">• x86 system server SP

Before You Begin

- Ensure that the Storage Monitoring feature is supported on your Oracle server. For details, see the ILOM Supplement guide or Platform Administration guide for your server.
- For Oracle servers supporting the Storage Monitoring feature, you must download and install a system management pack prior to using the Storage Monitoring features in ILOM. For information about how to download this management pack, see *Sun Server Hardware Management Pack User's Guide* (821-1609).
- You must be using ILOM 3.0.8 or a later version of ILOM.
- Some Oracle servers might not enable support for the storage monitoring functions that are described in this chapter. To determine whether storage monitoring support on your server has been enabled, see the ILOM Supplement guide or Platform Administration guide for your server.
- For Oracle servers supporting the Storage Monitoring feature in ILOM, a system management pack must be installed to use the Storage Monitoring features. For information about how to download this management pack, see *Oracle Server Hardware Management Pack User's Guide* (821-1609).
- For conceptual information and examples on viewing and monitoring storage components, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410).

▼ View and Monitor RAID Controller Details

1. Log in to the ILOM SP web interface.
2. In the ILOM web interface, click the Storage --> RAID --> Controllers tab.
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

Show Topology

	Controller Name	RAID Levels	Max Disks	Max RAIDs
<input type="radio"/>	controller@0d:00.0	0, 1, 1E	63	2
<input type="radio"/>	controller@0d:00.1	0, 1, 1E	63	2

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.

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_spare	0
max_global_hot_spare	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

1. Log in to the ILOM SP web interface.
2. In the ILOM web interface, click the Storage --> RAID --> Disks tab.

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

RAID

Controllers Disks Volumes

Disk Monitoring

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

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.

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

1. Log in to the ILOM SP web interface.

2. In the ILOM web interface, click the Storage --> RAID --> Volumes tab.

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

The screenshot shows the RAID Volumes monitoring page. At the top, there are tabs for 'RAID', 'Controllers', 'Disks', and 'Volumes'. Below the tabs is the 'Volume Monitoring' section, which includes a sub-header 'Volume Info' and a table listing RAID volumes. The table has five columns: Volume Name, Status, RAID Level, Capacity (GB), and Device Name. Three volumes are listed: controller@0d:00.0/raid_id4, controller@0d:00.0/raid_id5, and controller@0d:00.1/raid_id6. The first volume is highlighted with a blue border.

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.

The screenshot shows a dialog box titled 'controller@0d:00.0/raid_id4'. It contains a table with two columns: 'Property' and 'Value'. The table lists four properties: level, status, disk_capacity, and device_name, with their corresponding values: 1, OK, 135, and /dev/sde.

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

Enabling or Disabling Zone Manager

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

Managing System Alerts

Topics

Description	Links
Review the prerequisites	<ul style="list-style-type: none"> • “Before You Begin” on page 98
Manage alert rule configurations	<ul style="list-style-type: none"> • “Create or Edit Alert Rules” on page 99 • “Disable an Alert Rule” on page 100
Generate test alert to confirm alert configuration is working	<ul style="list-style-type: none"> • “Generate Test Alerts” on page 100
Send a test email alert before saving an alert rule	<ul style="list-style-type: none"> • “Send Test Email Alert to Specific Alert Destination” on page 101
Notify recipient of system alerts using email	<ul style="list-style-type: none"> • “Enable SMTP Client” on page 102
Download SNMP MIBs directly from ILOM	<ul style="list-style-type: none"> • “Download SNMP MIBs” on page 103

Related Topics

For ILOM	Chapter or Section	Guide
<ul style="list-style-type: none"> • Concepts 	<ul style="list-style-type: none"> • System Monitoring and Alert Management 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide</i> (820-6410)
<ul style="list-style-type: none"> • CLI 	<ul style="list-style-type: none"> • Managing System Alerts 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide</i> (820-6412)

The ILOM 3.0 Documentation Collection is available at:

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

Related Topics

For ILOM	Chapter or Section	Guide
• SNMP	• Managing Alerts	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference</i> (820-6413)

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

Managing Alert Rule Configurations

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• “Before You Begin” on page 98	• x86 system server SP • SPARC system server SP
Manage alert rule configurations	• “Create or Edit Alert Rules” on page 99 • “Disable an Alert Rule” on page 100 • “Generate Test Alerts” on page 100 • “Send Test Email Alert to Specific Alert Destination” on page 101	• CMM

Before You Begin

- If you are defining an Email Notification alert, the outgoing email server that will be used to send the email notification must be configured in ILOM. If an outgoing email server is not configured, ILOM will not be able to successfully generate Email Notification alerts.
- If you are defining an SNMP Trap alert with the version set to SNMP v3, the SNMP user name must be defined in ILOM as an SNMP user. If the user is not defined in ILOM as an SNMP user, the SNMP user will be unable to decode the SNMP alert message.

- If you are using a modular chassis system, you can manage alert rule configurations for a server SP from the CMM web interface. To manage alert rule configuration for a server SP from the CMM, select the server SP (blade) in the left frame of the page, then in the right frame of the page, click Configuration -->Alert Management.
- To manage alert rule configurations, you need the Admin (a) role enabled.
- To send a test email alert, you need the Read Only (o) role enabled and you must be using ILOM 3.0.4 or a later version of ILOM.

▼ Create or Edit Alert Rules

Follow these steps to configure alert rules:

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select 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, and SNMP Traps click *Edit* to configure an alert. You can configure up to 15 alerts.

Alert ID	Level	Alert Type	Destination Summary
<input type="radio"/> 1	disable	ipmipet	0.0.0.0
<input type="radio"/> 2	disable	ipmipet	0.0.0.0
<input type="radio"/> 3	disable	ipmipet	0.0.0.0
<input type="radio"/> 4	disable	ipmipet	0.0.0.0

3. In the Alert Settings page, do the following:
 - a. Select the radio button for alert rule you want to create or edit.
 - b. In the Actions drop-down 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 an SNMP Trap, then you can optionally define a community name or user name value for authenticating the receipt of the alert message.

For more information about the property values you can specify for an alert rule, see “About Alert Management” in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

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

▼ Disable an Alert Rule

Follow these steps to disable an alert rule:

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Select Configuration --> Alert Management.**
The Alert Settings page appears.
3. **In the Alert Settings page, select the radio button for the alert rule you want to disable then select Edit in the Actions drop-down list box.**
A dialog appears presenting properties you can define about the alert rule.
4. **In the properties dialog box, select Disabled in the Alert Levels drop-down list box.**
5. **Click Save to apply the value specified and to close the properties dialog.**

▼ Generate Test Alerts

Follow these steps to generate test alerts:

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Select Configuration --> Alert Management.**
The Alert Settings page appears.
3. **In the Alert Settings page, click the Send Test Alert button.**
ILOM generates test alerts to each of the alert rule configurations enabled on the Alert Settings page.

▼ Send Test Email Alert to Specific Alert Destination

Follow these steps to send a test email alert:

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Select Configuration --> Alert Management.**
The Alert Settings page appears.
3. **In the Alert Settings page, perform the following steps to send a test email alert:**
 - a. **Select the radio button of the alert rule.**
 - b. **Click the Test Rule button to send a text email alert to the alert rule destination.**

Configuring SMTP Client for Email Notification Alerts

Topics

Description	Links	Platform Feature Support
Notify recipient of system alerts using email	<ul style="list-style-type: none">• "Enable SMTP Client" on page 102	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

- To enable SMTP Clients, you need the Admin (a) role enabled.
- To generate configured Email Notification alerts, you must enable the ILOM client to act as an SMTP client to send the email alert messages.
- Prior to enabling the ILOM client as an SMTP client, determine the IP address and port number of the outgoing SMTP email server that will process the email notification.

▼ Enable SMTP Client

Follow these steps to enable an SMTP client:

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Select 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	Select this check box to enable this state.
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.**

Downloading SNMP MIBs Directly From ILOM

Topics

Description	Links	Platform Feature Support
Download SNMP MIBs directly from ILOM	<ul style="list-style-type: none">• "Download SNMP MIBs" on page 103	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

- The Reset and Host Control (r) role is required to download SNMP MIBs from ILOM.
- You must be using ILOM 3.0.4 or a later version of ILOM.

▼ Download SNMP MIBs

Follow these steps to download SNMP MIBs:

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

2. Click Configuration --> System Management Access --> SNMP.

The SNMP Management page appears.

3. Click the MIBs jump link, or scroll down to the MIBs section.

The MIBs section of the page appears.

MIBs

The ILOM MIBs may be downloaded directly from the SP for use with an SNMP management application.

[Download](#)

[^ Back to Top](#)

4. Click Download, then click Save and enter the destination to save the file.

A zip file containing the MIBs are transferred to the destination server.

Power Monitoring and Management of Hardware Interfaces

Topics

Description	Links
Identify Power Monitoring and Management feature updates per ILOM firmware point release	<ul style="list-style-type: none">• “Summary of Power Management Feature Updates” on page 106
Web procedures for power monitoring and management of hardware interfaces	<ul style="list-style-type: none">• “Monitoring System Power Consumption” on page 109• “Configuring Power Policy Settings to Manage Server Power Usage” on page 113• “Configuring Power Consumption Threshold Notifications” on page 117• “Monitoring and Configuring Component Power Allocation Distributions” on page 118• “Configuring Server Power Limit Properties” on page 126• “Monitoring or Configuring CMM Power Supply Redundancy Properties” on page 130

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Power Monitoring and Management of Hardware Interfaces	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
• CLI	• Power Monitoring and Management of Hardware Interfaces	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>
• SNMP	• Power Monitoring and Management of Hardware Interfaces	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide (820-6413)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Summary of Power Management Feature Updates

TABLE 9-1 identifies the common power management feature enhancements and documentation updates made since ILOM 3.0.

TABLE 9-1 Power Management Feature Updates per ILOM Firmware Point Release

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Updated Web Procedures, See:
Monitor Power Consumption Metrics	ILOM 3.0	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• “Monitoring System Power Consumption” on page 109
Configure Power Policy Properties	ILOM 3.0	<ul style="list-style-type: none">• New power policy properties explained.• New CLI and web procedures added for configuring power policy settings	<ul style="list-style-type: none">• “Configuring Power Policy Settings to Manage Server Power Usage” on page 113

TABLE 9-1 Power Management Feature Updates per ILOM Firmware Point Release (Continued)

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Updated Web Procedures, See:
Monitor Power Consumption History	ILOM 3.0.3	<ul style="list-style-type: none"> • New power consumption history metrics • New CLI and web procedures added for monitoring power consumption 	<ul style="list-style-type: none"> • “Monitor Power Statistics and Power History” on page 111
Configure Power Consumption Notification Thresholds	ILOM 3.0.4	<ul style="list-style-type: none"> • New power consumption notification threshold settings • New CLI and web procedures added for configuring the power consumption thresholds 	<ul style="list-style-type: none"> • “Configuring Power Consumption Threshold Notifications” on page 117
Monitor Allocation Power Distribution Metrics	ILOM 3.0.6	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • “Monitoring and Configuring Component Power Allocation Distributions” on page 118
Configure Power Budget Properties	ILOM 3.0.6	<ul style="list-style-type: none"> • New power budget properties • New CLI and web procedures added for configuring power budget properties 	<ul style="list-style-type: none"> • “Configuring Server Power Limit Properties” on page 126
Configure Power Supply Redundancy Properties for CMM Systems	ILOM 3.0.6	<ul style="list-style-type: none"> • New power supply redundancy properties for CMM systems • New CLI and web procedures added for configuring power supply redundancy properties on CMM systems 	<ul style="list-style-type: none"> • “Monitoring or Configuring CMM Power Supply Redundancy Properties” on page 130
Server Power Allocation Tab Replaces Distribution Tab	ILOM 3.0.8	<ul style="list-style-type: none"> • ILOM web Allocation tab replaces Distribution tab for server SPs • New web procedure added for viewing server power allocation properties 	<ul style="list-style-type: none"> • “Monitoring and Configuring Component Power Allocation Distributions” on page 118
Server Limit Tab Replaces Budget Tab	ILOM 3.0.8	<ul style="list-style-type: none"> • ILOM web Limit tab replaces Budget tab for server SPs • New web procedure added for configuring power limit properties 	<ul style="list-style-type: none"> • “Configuring Server Power Limit Properties” on page 126

TABLE 9-1 Power Management Feature Updates per ILOM Firmware Point Release *(Continued)*

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Updated Web Procedures, See:
Web Interface Layout Update for CMM Power Management	ILOM 3.0.10	<ul style="list-style-type: none">• New top-level tab added to ILOM web interface for Power Management• Revised ILOM web Power Consumption tab properties for CMMs• ILOM web Allocation tab replaces Distribution tab for CMMs• Power Management Metrics tab removed from CMM ILOM web interface• Updated web procedure for configuring a grant limit for blade slots (previously known as allocatable power)	<ul style="list-style-type: none">• “Monitor System Power Consumption” on page 110• “View CMM Component Power Allocations” on page 121• “Configure Grant Limit for Blade Slots in CMM as of ILOM 3.0.10” on page 125• “View CMM Component Power Allocations” on page 121
Power Management Statistic tab	ILOM 3.0.14	<ul style="list-style-type: none">• The Power Statistics table on the History tab was moved to a Power Management --> Statistics tab	<ul style="list-style-type: none">• “Monitor Power Statistics and Power History” on page 111

Monitoring System Power Consumption

c

Topics

Description	Links	Platform Feature Support
Monitor power consumption	<ul style="list-style-type: none">• “Monitor System Power Consumption” on page 110• “Monitor Individual Power Supply Consumption” on page 111	<ul style="list-style-type: none">• x86 server SP• SPARC servers• CMM
Monitor power consumption history	<ul style="list-style-type: none">• “Monitor Power Statistics and Power History” on page 111	<ul style="list-style-type: none">• x86 server SP• SPARC servers• CMM

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- Review the web interface enhancements described in the section about system Power Consumption Metrics in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

Note – The power consumption features described in this chapter might not be implemented on 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 ILOM Supplement or Administration guide provided for your server.

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

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

▼ Monitor System Power Consumption

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

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

- If you are using ILOM 3.0.3 or later, select Power Management --> Consumption.
- If you are running ILOM firmware prior to ILOM 3.0.3, select System Monitoring --> Power Management.

The Power Consumption page appears.

Note – The ability to monitor power varies depending on server platform implementation of this feature. Refer to the platform-specific ILOM Supplement or Platform Administration guide for details and procedures.

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

Note – The properties on the Power Consumption page were updated for server SPs as of ILOM 3.0.8 and CMMs as of ILOM 3.0.10. For more information about these properties, refer to the section about Web Enhancements for Power Metrics in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

System Information	System Monitoring	Power Management	Configuration	User Management	Re
Consumption	Limit	Allocation	History		

Power Consumption

View actual system input power consumption, power consumption limit, and configure notification thresholds from this page. An I 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
 watts
 The default is: Disabled (0)

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

▼ Monitor Individual Power Supply Consumption

- For instructions on viewing sensors, refer to [“View Sensor Readings”](#) on page 80.

▼ Monitor Power Statistics and Power History

1. Log in to server SP or CMM ILOM web interface.
2. In the ILOM web interface, do one of the following:
 - If you are running ILOM firmware prior to ILOM 3.0.3, select System Monitoring --> Power Management then click the Power History link.
 - If you are using ILOM 3.0.3 or later, select Power Management -->History.
 - If you are using ILOM 3.0.14 or later, select Power Management -->Statistics to view the power statistics or select Power Management -->History to view the power history.

Refer to the section about Power Monitoring Terminology in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* for a description of these power monitoring history terms.

Note – The Statistic table available on the History tab as of ILOM 3.0.3 was moved to the Statistic tab in ILOM 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/PS	1400.000	1400.000	1400.000
/CH/BL0/PS	No Data	No Data	No Data
/CH/BL1/PS	No Data	No Data	No Data
/CH/BL2/PS	No Data	No Data	No Data
/CH/BL3/PS	No Data	No Data	No Data
/CH/BL4/PS	No Data	No Data	No Data
/CH/BL5/PS	No Data	No Data	No Data
/CH/BL6/PS	No Data	No Data	No Data
/CH/BL7/PS	No Data	No Data	No Data
/CH/BL8/PS	10.000	10.000	10.000
/CH/BL9/PS	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/PS	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/PS	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/PS	0 (1 Minute Average, 1 Hour History)	No Data	No Data	No Data	1 Minute Average	1 Hour History

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

Configuring Power Policy Settings to Manage Server Power Usage

Topics

Description	Links	Platform Feature Support
Configure policy to control power consumption	<ul style="list-style-type: none">• “Configure Power Consumption Policy” on page 114	<ul style="list-style-type: none">• x86 server SP (prior to ILOM 3.0.4)• SPARC servers
Configure policy to control power capping	<ul style="list-style-type: none">• “Configure Server Power Policy Ffor Power Capping” on page 115	<ul style="list-style-type: none">• x86 server SP• SPARC servers

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- Review the web interface enhancements described in the section about Power Policy Settings in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

Note – The power policy 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 ILOM Supplement or Administration guide provided for your server.

- To configure the Power Consumption Policy properties in ILOM for x86 servers, you must have Administrator (a) role privileges and you must be running ILOM 3.0.3 or earlier.
- To configure the Power Consumption Policy properties in ILOM for SPARC servers, you must have Administrator (a) role privileges and you must be running ILOM 3.0 or later.
- To configure the policy for powering capping on the Limit tab of the web interface, you must have Administrator (a) role privileges and you must have ILOM 3.0.8 or later installed on your server.

▼ Configure Power Consumption Policy

1. Log in to the server SP web interface.

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

- If you are using ILOM 3.0.3 or earlier, select System Monitoring --> Power Management to view the Power Policy settings.
- If you are using ILOM 3.0.4 or later on a SPARC server, select Power Management --> Settings to view the Power Policy settings.

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

3. In the Power Policy list box select 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% at all times, even if workload fluctuates.

The screenshot displays the ILOM web interface navigation menu at the top, with tabs for System Information, System Monitoring, Configuration, User Management, Remote Control, and Maintenance. Under System Monitoring, there are sub-tabs for Sensor Readings, Indicators, Event Logs, and Power Management. The main content area is titled "Power Management" and includes a sub-header "Consumption" with the following data: Actual Power: 0.00 watts, Permitted Power: 762 watts, and Available Power: 762 watts. Below this is a "Settings" section with a "Power Policy" dropdown menu currently set to "Performance" and a "Save" button.

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

4. Click **Save** to apply the new setting.

▼ Configure Server Power Policy Ffor Power Capping

1. Log in to the server SP ILOM web interface.
2. In the ILOM web interface, select the Power Management --> Limit tabs.
3. In the Power Limit page, configure the Policy settings for power capping as described below.

Property	Description
Policy	<p>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:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> - System Default – Platform selected optimum grace period. <i>or</i> - Custom – User-specified grace period. • Hard - Fixed cap keeps Peak Permitted power under Target Limit. – If you enable this option, power capping is permanently applied without a grace period.
Violation Actions	<p>The Violation Actions property enables you to specify the settings you want ILOM to take if the power limit cannot be achieved within the set grace period.</p> <p>You can choose to specify one of the following actions:</p> <ul style="list-style-type: none"> • None – If you enable this option and the power limit cannot be achieved, ILOM will display a Status Error Message to notify you that ILOM is unable to achieve the power capping limit specified. <p><i>or</i></p> <ul style="list-style-type: none"> • Hard-Power-Off – If you enable this option and the power limit cannot be achieved, ILOM takes the following actions: <ul style="list-style-type: none"> * Display a Status Error Message. * Initiates a hard-power-off of the server. <p>Note - The default option for Violation Actions is None.</p>

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

Topics

Description	Links	Platform Feature Support
View or configure power consumption notification thresholds	<ul style="list-style-type: none">• “View and Configure Notification Thresholds Using the Web Interface” on page 117	<ul style="list-style-type: none">• x86 servers• SPARC servers• CMM

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- You must have ILOM 3.0.4 or later installed on your server or CMM.
- You must have Administrator (a) privileges in ILOM to change power consumption configuration variables.

▼ View and Configure Notification Thresholds Using the Web Interface

1. Log in to server SP or CMM ILOM web interface.
2. In the web interface page, click Power Management --> Consumption.
The Power Consumption page appears.
3. In the Power Consumption page, do the following:
 - a. In the Notification Threshold field, select the Enabled check box.
 - b. Based on your platform requirements, specify a notification threshold value in the Watts text box.
 - c. Click Save to apply these changes.

Monitoring and Configuring Component Power Allocation Distributions

Topics

Description	Links	Platform Feature Support
View component allocation metrics for server or CMM	<ul style="list-style-type: none">• "View Server Component Power Allocations" on page 119• "View CMM Component Power Allocations" on page 121	<ul style="list-style-type: none">• x86 servers• SPARC servers• CMM
Configure permitted power for blade slots in chassis	<ul style="list-style-type: none">• "Configure Permitted Power for Blade Slots in CMM as of ILOM 3.0.6" on page 124• "Configure Grant Limit for Blade Slots in CMM as of ILOM 3.0.10" on page 125	<ul style="list-style-type: none">• CMM

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- Review the conceptual information about Component Allocation Power Distribution in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- You must have ILOM 3.0.6 or later installed on your server SP or CMM. Where noted, some procedures described in this section require the server SP or CMM to be running ILOM 3.0.10 or later.
- You must have administrator (a) privileges in ILOM to change any power consumption or allocation configuration variables.

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

▼ View Server Component Power Allocations

1. Log in to the ILOM SP web interface.
2. In the web interface, do one of the following:
 - If you are using ILOM 3.0.6, select the Power Management --> Distribution tabs.
 - If you are using ILOM 3.0.8 or later, select the Power Management --> Allocation tabs.

The Power Distribution or Power Allocation Plan page appears.

System Information	System Monitoring	Power Management	Configuration	User Management	Remote Control
Consumption	Limit	Allocation	History		

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 <i>Peak Permitted Power</i>

Per Component Power Map

Component	Allocated Power (Watts)	Can be C
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

3. In the allocation power table(s), 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 ILOM 3.0.8

1. Log in to the server SP ILOM web interface.
2. In the ILOM web interface, select the Power Management --> Limit tabs.

Note – The Power Management --> Distribution tab was renamed to Limit as of 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.
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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> - System Default – Platform selected optimum grace period. <i>or</i> - Custom – User-specified grace period. • 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.

Power Limit Property	Description
Violation Actions	<p>The Violation Actions property enables you to specify the settings you want ILOM to take if the power limit cannot be achieved within the set grace period.</p> <p>You can choose to specify one of the following actions:</p> <ul style="list-style-type: none"> • None – If you enable this option and the power limit cannot be achieved, ILOM will display a <i>Status Error Message</i> to notify you that ILOM is unable to achieve the power capping limit specified. <p><i>or</i></p> <ul style="list-style-type: none"> • Hard-Power-Off – If this option is chosen and the power limit cannot be achieved, ILOM takes the following actions: <ul style="list-style-type: none"> * Display a <i>Status Error Message</i>. * Initiates a hard-power-off of the server. <p>Note - The default option for Violation Actions is None.</p>

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

1. Log in to the ILOM CMM web interface.
2. In the left pane of the CMM web interface page, select CMM then do one of the following:
 - If you are running ILOM 3.0.6 or later, select the Power Management --> Distribution tabs.
 - If you are running ILOM 3.0.10 or later, select Power Management --> Allocation tabs.

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

The CMM Power Allocation Plan page appears.

System Information	System Monitoring	Power Management	Storage	Configuration	User Management	Remote Control	Maintenance
Consumption	Allocation	Redundancy	History				

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 <i>Power Supply Maximum</i> reserved by redundancy policy
Peak Permitted	6400	Maximum power the system is permitted to consume (redundancy policy is applied)
Allocated Power	3757	Sum of <i>Allocated Power</i> for chassis components and <i>Granted Power</i> 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	2543	Remaining power the system can grant to blades without exceeding <i>Peak Permitted</i>
Unfilled Grant Requests	1356	Sum of <i>Required Power</i> for blades that have not yet been granted power

Blade Power Grants				
<input type="button" value="Edit"/>				
	Blade Slot	Grant Limit (Watts)	Required Power (Watts)	Granted Power (Watts)
-	TOTAL	-	1919 (total)	563 (total)
<input type="radio"/>	0	1200	183	183
<input type="radio"/>	1	800	Empty Slot	-
<input type="radio"/>	2	1100	Empty Slot	-
<input type="radio"/>	3	1200	Empty Slot	-
<input type="radio"/>	4	1200	234	234
<input type="radio"/>	5	1200 (ignored - auto-powered I/O blade)	146	146
<input type="radio"/>	6	1200	389	0
<input type="radio"/>	7	1200	371	0
<input type="radio"/>	8	1200	371	0
<input type="radio"/>	9	1200	225	0

Chassis Component Slot Power Map	
Component	Allocated Power (Watts)
TOTAL	3156 (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
PSU_FAN0	18
PSU_FAN1	18

3. In the CMM Power Allocation Page page, view the power allocation values.
- For ILOM 3.0.6 or later these CMM power allocation values appear as:

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: <ul style="list-style-type: none"> • 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. <p>Note - To modify the Permitted Power allocated to a server module slot, see "Configure Permitted Power for Blade Slots in CMM as of ILOM 3.0.6" on page 124.</p>
Component Power Distribution	View allocated power for each non-blade component in the system.

- For ILOM 3.0.10 or later these CMM power allocation values appear as:

Updated Property Name	Details
Grantable Power (renamed property)	Allocatable Power in ILOM 3.0.6 was renamed to Grantable Power in ILOM 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 ILOM 3.0.6 was renamed to Grant Limit in ILOM 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 ILOM 3.0.6" on page 124.
Granted Power (renamed property)	Allocated Power in ILOM 3.0.6 was renamed to Granted Power in ILOM 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 ILOM 3.0.6

1. Log in to the ILOM CMM web interface.
2. In the left pane of the web interface page, select CMM then select the Power Management --> Distribution tabs.
3. Scroll down to the Blade Slot Power Distribution table.

Blade Slot	Allocated Power (Watts)	Permitted Power (Watts)
- Blade Slots (total)	3175	-
<input type="radio"/> BL0	435	1200
<input type="radio"/> BL1	410	1000
<input type="radio"/> BL2	268	1200
<input type="radio"/> BL3	309	1200
<input type="radio"/> BL4	268	1200
<input type="radio"/> BL5	506	1200
<input type="radio"/> BL6	146	1200
<input type="radio"/> BL7	265	1200
<input type="radio"/> BL8	300	1200
<input type="radio"/> BL9	268	1200

4. In the Blade Slot Power Distribution table, do the following.
 - a. Select the radio button for the blade slot Permitted Power allocation 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: watts

- c. In the dialog, modify the Permitted Power value, 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 ILOM 3.0.10

1. Log in to the CMM ILOM web interface.

Note – To change any power property value for blade slots in ILOM requires an Admin (a) role user account.

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

The CMM Power Allocation page appears.

3. Scroll down to the Blade Slot Grants table.

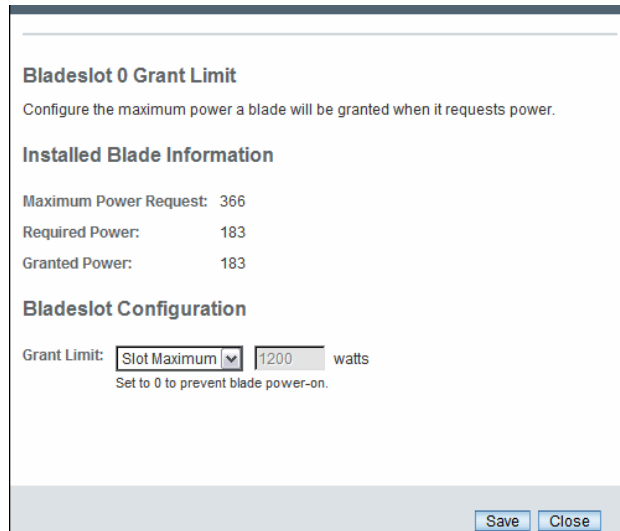
Blade Power Grants				
<input type="button" value="Edit"/>				
<input type="checkbox"/>	Blade Slot	Grant Limit (Watts)	Required Power (Watts)	Granted Power (W)
-	TOTAL	-	1919 (total)	952 (total)
<input type="radio"/>	0	1200	183	183
<input type="radio"/>	1	800	Empty Slot	-
<input type="radio"/>	2	1100	Empty Slot	-
<input type="radio"/>	3	1200	Empty Slot	-
<input type="radio"/>	4	1200	234	234
<input type="radio"/>	5	1200 (ignored - auto-powered I/O blade)	146	146
<input type="radio"/>	6	1200	389	389
<input type="radio"/>	7	1200	371	0
<input type="radio"/>	8	1200	371	0
<input type="radio"/>	9	1200	225	0

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

a. Select the radio button for the blade slot that you want to modify.

b. Click Edit.

A dialog appears listing power configuration information for the blade.



- c. In the dialog, modify the Grant Limit value by selecting Custom and specifying a value for the wattage, then click Save.

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

Configuring Server Power Limit Properties

Topics

Description	Links	Platform Feature Support
Configure server SP power limit properties	<ul style="list-style-type: none"> "Configure Server Power Limit Properties" on page 127 	<ul style="list-style-type: none"> x86 servers SPARC servers

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

- Review the conceptual information about Server Power Limit (or Server Power Budget) in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- You must have ILOM 3.0.6 or later installed on your server to configure the server power limit properties.
- You must have administration (a) privileges in ILOM to change any power management configuration variables.

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

▼ Configure Server Power Limit Properties

1. Log in to the server SP ILOM web interface.
2. In the ILOM web interface, do one of the following:
 - If you are using ILOM 3.0.6, select the Power Management --> Budget tabs.
 - If you are using ILOM 3.0.8 or later, select the Power Management --> Limit tabs.

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

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 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 - Target Limit was previously named Power Limit on the Budget tab in ILOM 3.0.6 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	<p>The Status Error Message read-only property only appears on the Limit page when ILOM fails to achieve the power limit that was configured.</p> <p>Note - The Status Error Message read-only property was previously named Status on the Budget tab in ILOM 3.0.6</p>
Policy	<p>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:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> - System Default – Platform-selected optimum grace period. <i>or</i> - Custom – User-specified grace period. • 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. <p>Note - The Policy was previously named Time Limit on the Budget tab in ILOM 3.0.6.</p>
Violation Actions	<p>The Violation Actions property enables you to specify the settings you want ILOM to take if the power limit cannot be achieved within the set grace period.</p> <p>You can choose to specify one of the following actions:</p> <ul style="list-style-type: none"> • None – If you enable this option and the power limit cannot be achieved, ILOM will display a Status Error Message to notify you that ILOM is unable to achieve the power capping limit specified. <p><i>or</i></p> <ul style="list-style-type: none"> • Hard-Power-Off – If you enable this option and the power limit cannot be achieved, ILOM takes the following actions: <ul style="list-style-type: none"> * Display a Status Error Message. * Initiates a hard-power-off of the server. <p>Note - The default option for Violation Actions is None.</p>

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 Properties

Topics

Description	Links	Platform Feature Support
Monitor or configure the CMM power supply redundancy properties	<ul style="list-style-type: none">• “View or Configure CMM Power Supply Redundancy Properties” on page 130	<ul style="list-style-type: none">• CMM

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- Review the conceptual information about power supply redundancy for CMM systems in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- You must have ILOM 3.0.6 or later installed on your server to configure the CMM power supply redundancy properties.
- You must have Administrator (a) role privileges in ILOM to change any power management configuration variables.

▼ View or Configure CMM Power Supply Redundancy Properties

1. Log in to the ILOM CMM web interface.
2. In the left pane of the CMM web interface, select CMM then in the right pane of the web interface page, select the Power Management --> Redundancy tabs. 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. Click Save to apply any changes made.

Backing Up and Restoring ILOM Configuration

Topics

Description	Links
Back up the ILOM configuration	<ul style="list-style-type: none">• “Back Up the ILOM Configuration” on page 134
Restore the ILOM configuration	<ul style="list-style-type: none">• “Restore the ILOM Configuration” on page 137
Reset ILOM configuration to default settings	<ul style="list-style-type: none">• “Reset the ILOM Configuration to Defaults” on page 142

Related Topics

For ILOM	Chapter or Section	Guide
<ul style="list-style-type: none">• Concepts	<ul style="list-style-type: none">• Configuration Management and Firmware Updates	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none">• CLI	<ul style="list-style-type: none">• Backing Up and Restoring ILOM Configuration	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Backing Up the ILOM Configuration

Topics

Description	Links	Platform Feature Support
Back up the ILOM configuration	<ul style="list-style-type: none">• "Back Up the ILOM Configuration" on page 134	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

Before You Begin

- To back up the ILOM configuration you need the Admin (a), User Management (u), Console (c), Reset and Host Control (r), and Read Only (o) roles enabled.
- If you use a user account that does *not* have the roles listed above, the configuration backup file created might not include all of the ILOM SP configuration data.

▼ Back Up the ILOM Configuration

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select Maintenance --> Backup/Restore.

The Configuration Backup/Restore page appears.

The screenshot shows the ILOM web interface navigation menu with tabs for System Information, System Monitoring, Power Management, Configuration, User Management, Remote Control, and Maintenance. The Maintenance tab is selected, showing sub-tabs for Firmware Upgrade, Backup/Restore, Configuration Management, Reset SP, and Snapshot. The main content area is titled "Configuration Backup/Restore" and contains instructions: "Perform system configuration backup or restore from this page. Select Backup or Restore from Operation menu. Choose a Transfer Method and fill in all required fields. You may ch data within a backup file or for decrypting such data when restoring a configuration. If a passphrase is not specified, then sensitive data will not be included in the backup file. Click /". Below the instructions is a form with two dropdown menus: "Operation:" set to "Backup" and "Transfer Method:" set to "Browser". A note states: "The downloaded file will be saved according to your browser settings." At the bottom of the form are two text input fields labeled "Passphrase:" and "Confirm Passphrase:".

3. Select **Backup** from the **Operation** drop-down list.

4. Select a transfer method from the **Transfer Method** drop-down list.


The following transfer methods are available:

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

5. If you select the **Browser** transfer method, the backup file is saved according to your browser settings.

6. If you select the **TFTP** transfer method, the prompts shown in the following figure appear and you must provide the following information:

- **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`.



The image shows a configuration form with the following elements:

- Operation:** A dropdown menu with "Backup" selected.
- Transfer Method:** A dropdown menu with "TFTP" selected.
- Host:** An empty text input field.
- Filepath:** An empty text input field.

7. If you select the **SCP, FTP, SFTP, HTTP, or HTTPS** transfer method, the prompts shown in the following figure appear and you must provide the following information:

- **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.

Operation:	<input type="text" value="Backup"/>
Transfer Method:	<input type="text" value="SCP"/>
Host:	<input type="text"/>
Filepath:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="text"/>

8. If you want sensitive data, such as passwords, SSH keys, certificates, and so forth, to be backed up, you must provide a passphrase. Type a passphrase in the Passphrase field and confirm the passphrase in the Confirm Passphrase field.

If you do not type a passphrase, sensitive data will not be backed up.

9. To initiate the backup operation, click Run.

The Backup operation is executed.

Note – While the Backup operation is executing, sessions on the ILOM SP will be momentarily suspended. The sessions will resume normal operation once the Backup operation is complete. A Backup operation typically takes two to three minutes to complete.

Restoring the ILOM Configuration

Topics

Description	Links	Platform Feature Support
Restore the ILOM configuration	<ul style="list-style-type: none"> • "Restore the ILOM Configuration" on page 137 • "Edit the Backup XML File" on page 139 	<ul style="list-style-type: none"> • x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To restore the ILOM configuration you need the Admin (a), User Management (u), Console (c), Reset and Host Control (r), and Read Only (o) roles enabled.

- If you use a user account that does not have the roles listed above, some of the information in the configuration file might not be restored. When executing a Restore operation, use a user account that has the same or more privileges than the user account that was used to create the backup file; otherwise, some of the backed up configuration data might not be restored. All configuration properties that are not restored appear in the event log. Therefore, you can verify whether all the configuration properties were restored by checking the event log.

▼ Restore the ILOM Configuration

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

2. **Select Maintenance --> Backup/Restore.**

The Configuration Backup/Restore page appears.

3. **Select Restore from the Operation drop-down list.**

The Configuration Backup/Restore page used for Restore operations appears.

4. **Select the transfer method from the Transfer Method drop-down list.**

The following transfer methods are available:

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

5. **If you select the Browser transfer method, type the directory path and file name for the backup file or click the Browse button to determine the backup file location.**

6. **If you select the TFTP transfer method, the prompts shown in the following figure appear and you must provide the following information:**

- **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`.

Operation:	<input type="text" value="Restore"/>
Transfer Method:	<input type="text" value="TFTP"/>
Host:	<input type="text"/>
Filepath:	<input type="text"/>

7. If you select the SCP, FTP, SFTP, HTTP, or HTTPS transfer method, the prompts shown in the following figure appear and you must provide the following information:

- **Host** – Enter the remote host IP address or, if you have DNS configured, the name of the remote host.
- **Filepath** – Enter the path to for 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.

Operation:	<input type="text" value="Restore"/>
Transfer Method:	<input type="text" value="SCP"/>
Host:	<input type="text"/>
Filepath:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="text"/>

8. If a passphrase was provided when the backup file was created, type the passphrase in the Passphrase field and confirm it in the Confirm Passphrase field.

The passphrase must be the same passphrase that was used when the backup file was created.

9. To initiate the Restore operation, click Run.

The Restore operation executes.

Note – While the Restore operation is executing, sessions on the ILOM SP will be momentarily suspended. The sessions will resume normal operation once the Restore operation is complete. A Restore operation typically takes two to three minutes to complete.

▼ Edit the Backup XML File

Before You Begin

- Before you use a backed up XML file on another system, you should edit the file to remove any information that is unique to a particular system, for example, the IP address.

The following is an example of a backed up XML file. The content of the file is abbreviated for this procedure.

```
<SP_config version="3.0">
  <entry>
    <property>/SP/check_physical_presence</property>
    <value>>false</value>
  </entry>
  <entry>
    <property>/SP/hostname</property>
    <value>labysystem12</value>
  </entry>
  <entry>
    <property>/SP/system_identifier</property>
    <value>SUN BLADE X8400 SERVER MODULE, ILOM v3.0.0.0, r32722
  </value>
  </entry>
  .
  .
  .
  <entry>
    <property>/SP/clock/datetime</property>
    <value>Mon May 12 15:31:09 2008</value>
  </entry>
  .
  .
  .
  <entry>
    <property>/SP/config/passphrase</property>
    <value encrypted="true">89541176be7c</value>
  </entry>
  .
  .
  .
  <entry>
    <property>/SP/network/pendingipaddress</property>
    <value>1.2.3.4</value>
  </entry>
  .
  .
  .
```

```

<entry>
<property>/SP/network/commitpending</property>
<value>>true</value>
</entry>
.
.
.
<entry>
<property>/SP/services/snmp/sets</property>
<value>enabled</value>
</entry>
.
.
.
<entry>
<property>/SP/users/john/role</property>
<value>aucro</value>
</entry>
<entry>
<entry>
<property>/SP/users/john/password</property>
<value encrypted="true">c21f5a3df51db69fdf</value>
</entry>
</SP_config>

```

1. Consider the following in the example XML file:

- The configuration settings, with exception of the password and the passphrase, are in clear text.
- The `check_physical_presence` property, which is the first configuration entry in the file, is set to `false`. The default setting is `true` so this setting represents a change to the default ILOM configuration.
- The configuration settings for `pendingipaddress` and `commitpending` are examples of settings that should be deleted before you use the backup XML file for a Restore operation because these settings are unique to each server.
- The user account `john` is configured with the `a, u, c, r, o` roles. The default ILOM configuration does *not* have any configured user accounts so this account represents a change to the default ILOM configuration.
- The SNMP `sets` property is set to `enabled`. The default setting is `disabled`.

2. To modify the configuration settings that are in clear text, change the values or add new configuration settings.

For example:

- To change the roles assigned to the user john, change the text as follows:

```
<entry>
<property>/SP/users/john/role</property>
<value>auo</value>
</entry>
<entry>
```

- To add a new user account and assign that account the a,u,c,r,o roles, add the following text directly below the entry for user john:

```
<entry>
<property>/SP/users/bill/role</property>
<value>aucro</value>
</entry>
<entry>
```

- To change a password, delete the encrypted="true" setting and the encrypted password string and enter the password in plain text. For example, to change the password for the user john, change the text as follows:

```
<entry>
<property>/SP/users/john/password</property>
<value>newpassword</value>
</entry>
```

- 3. After you have made the changes to the backup XML file, save the file so that you can use it for a Restore operation on the same system or a different system.**

Resetting the ILOM Configuration

Topics

Description	Links	Platform Feature Support
Reset the ILOM configuration to default settings	<ul style="list-style-type: none">• "Reset the ILOM Configuration to Defaults" on page 142	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM

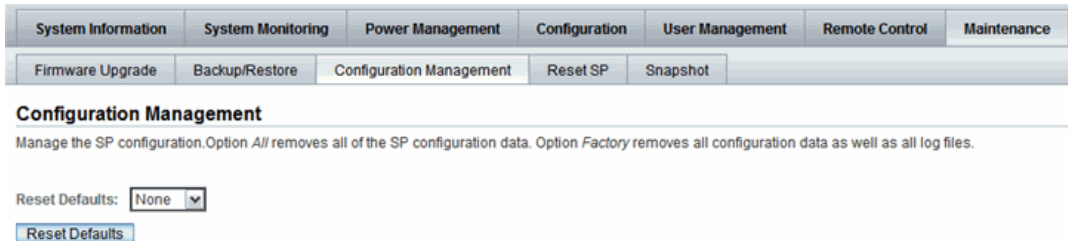
Before You Begin

- To reset the ILOM configuration to defaults, you need the Admin (a) role enabled.

▼ Reset the ILOM Configuration to Defaults

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Select Maintenance --> Configuration Management.

The Configuration Management page appears.



3. Select one of the following options in the Reset Defaults drop-down list, then click Reset Defaults.
 - All – If you want to reset all of the ILOM configuration data to the default settings with the exception of the log files, select All in the Reset Defaults drop-down list and click Reset Defaults. The next time the ILOM SP reboots, the configuration will be restored to the default settings.

- **Factory** – If you want to reset all of the ILOM configuration data to default settings and also erase the log files, select **Factory** in the **Reset Defaults** drop-down list and click **Reset Defaults**. The next time the ILOM SP reboots, the configuration will be restored to the default settings and the log files are erased.
- **None** – If you want to cancel the reset to defaults operation just previously issued, select **None** in the **Reset Defaults** drop-down list and click **Reset Defaults**. The previously issued reset to defaults operation is canceled provided the **None** option is executed before the ILOM SP reboots.

Updating ILOM Firmware

Topics

Description	Links
Review the prerequisites	<ul style="list-style-type: none"> • “Before You Begin” on page 146
Update ILOM firmware	<ul style="list-style-type: none"> • “Identify ILOM Firmware Version” on page 147 • “Download New ILOM Firmware Image” on page 147 • “Update the Firmware Image” on page 148 • “Recover From a Network Failure During Firmware Update” on page 149
Reset the ILOM SP	<ul style="list-style-type: none"> • “Reset ILOM SP” on page 150

Related Topics

For ILOM	Chapter or Section	Guide
<ul style="list-style-type: none"> • Concepts 	<ul style="list-style-type: none"> • Configuration Management and Firmware Updates 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none"> • CLI 	<ul style="list-style-type: none"> • Updating ILOM Firmware 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>
<ul style="list-style-type: none"> • IPMI and SNMP hosts 	<ul style="list-style-type: none"> • Configuring ILOM Firmware Settings 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide (820-6413)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Related Topics

For ILOM	Chapter or Section	Guide
• CLI and Web interface (CMM only)	• Firmware Update Procedures	<i>Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems</i> (820-0052)

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

Updating the Firmware

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• "Before You Begin" on page 146	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP
Update ILOM firmware	<ul style="list-style-type: none">• "Identify ILOM Firmware Version" on page 147• "Download New ILOM Firmware Image" on page 147• "Update the Firmware Image" on page 148• "Recover From a Network Failure During Firmware Update" on page 149	<ul style="list-style-type: none">• CMM

Before You Begin

Prior to performing the procedures in this section, the following requirements must be met:

- Identify the version of ILOM that is currently running on your system. For details, see ["Identify ILOM Firmware Version" on page 147](#)
- Download the firmware image for your server or CMM from the Oracle Sun download web site and place the image on your TFTP, FTP, or HTTP server.
- If required by your platform, shut down your host operating system before changing the firmware on your server SP.

- Obtain an ILOM user name and password that has Admin (a) role account privileges. You must have Admin (a) privileges to update the firmware on the system.
- The firmware update process takes several minutes to complete. During this time, do not perform other ILOM tasks. When the firmware update is complete, the system will reboot.

Note – As of ILOM 3.0.10, a new feature is available to manage firmware updates for Oracle Sun Modular System chassis components. For information and procedures for updating ILOM firmware on CMM chassis components, refer to the *Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems* (820-0052).

▼ Identify ILOM Firmware Version

Follow these steps to identify the firmware version:

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

The current firmware version information appears.

▼ Download New ILOM Firmware Image

1. **Navigate to <http://www.oracle.com/us/products/servers-storage/servers/index.html>**
2. **Expand the “Downloads” box at the right of the page, then click the “Drivers and Firmware” link.**
3. **Navigate to the appropriate page for your Sun server.**
4. **Select the “Downloads and Firmware” tab.**
5. **Click the “Download” link that is appropriate for your server.**

▼ Update the Firmware Image

Before You Begin

- If required by your platform, shut down your host operating system before updating the firmware on your server SP.
- To gracefully shut down your host operating system, use the Remote Power Controls -> Graceful Shutdown and Power Off option in the ILOM web interface, or issue the `stop /SYS` command from the ILOM CLI.

Follow these steps to update the firmware image:

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

2. Select Maintenance --> Firmware Upgrade.

The Firmware Upgrade page appears.

3. In the Firmware Upgrade page, click Enter Upgrade Mode.

An Upgrade Verification dialog appears, indicating that other users who are logged in will lose their session when the update process completes.

4. In the Upgrade verification dialog, click OK to continue.

The Firmware Upgrade page appears.

5. In the Firmware Upgrade page, perform the following actions:

a. Specify the image location by performing one of the following:

- Click Browse to select the location of the firmware image you want to install.
- If supported on your system, click Specify URL. Then type the URL that will locate the firmware image into the text box.

b. Click the Upload button to upload and validate the file.

Wait for the file to upload and validate.

The Firmware Verification page appears.

6. In the Firmware Verification page, enable any of the following options:

- **Preserve Configuration.** Enable this option if you want to save your existing configuration in ILOM and restore that existing configuration after the update process completes.
- **Delay BIOS upgrade until next server poweroff.** Enable this option if you want to postpone the BIOS upgrade until the next time the system reboots.

Note – The “Delay BIOS upgrade” option appears only for firmware updates to ILOM 3.0 or later on x86 systems.

Note – The BIOS default settings cannot be preserved when updating the SP firmware. After updating the SP firmware, the default settings are automatically loaded for the new BIOS image.

7. Click Start Upgrade to start the upgrade process or click Exit to cancel the process.

When you click Start Upgrade the upload process will start and a prompt to continue the process appears.

8. At the prompt, click OK to continue.

The Update Status page appears providing details about the update progress. When the update indicates 100%, the firmware upload is complete.

When the upload completes, the system *automatically* reboots.

Note – The ILOM web interface might not refresh properly after the update completes. If the ILOM web is missing information or displays an error message, you might be viewing a cached version of the page from the version previous to the update. Clear your browser cache and refresh your browser before continuing.

9. Reconnect to the SP (or CMM) ILOM web interface. Select System Information --> Version to verify that the firmware version on the SP or CMM corresponds to the firmware image you installed.

Note – If you did not preserve the ILOM configuration before the firmware update, you will need to perform the initial ILOM setup procedures to reconnect to ILOM.

▼ Recover From a Network Failure During Firmware Update

If you were performing the firmware update process via the ILOM web interface using a *local file* and a network failure occurs, ILOM will automatically time-out and reboot the system.

Follow these steps to recover from a network failure during firmware update:

- 1. Address and fix the network problem.**
- 2. Reconnect to the ILOM SP.**
- 3. Restart the firmware update process.**

Resetting ILOM SP

Topics

Description	Links	Platform Feature Support
Reset the ILOM SP	<ul style="list-style-type: none">• "Reset ILOM SP" on page 150	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP

Before You Begin

- To reset the SP, you need the Reset and Host Control (r) role enabled.
- After updating the ILOM/BIOS firmware, you must reset the ILOM SP.

▼ Reset ILOM SP

If you need to reset your ILOM service processor (SP), you can do so without affecting the host OS. However, resetting an SP disconnects your current ILOM session and renders the SP unmanageable during reset.

1. Log in to the ILOM SP web interface.

2. Select Maintenance --> Reset SP.

The Reset Service Processor page appears

3. Click the Reset SP button.

ILOM reboots. The web interface is unavailable while ILOM reboots.

Managing Remote Hosts Redirection and Securing the ILOM Remote Console

Topics

Description	Links
Perform initial setup for ILOM remote console	<ul style="list-style-type: none">• "Configure ILOM Remote Control Video Redirection Settings" on page 154
Redirect host devices using ILOM remote console	<ul style="list-style-type: none">• "Launch the Oracle ILOM Remote Console" on page 158• "Start, Stop, or Restart Device Redirection" on page 160• "Redirect Keyboard Input" on page 160• "Control Keyboard Modes and Key Send Options" on page 161• "Redirect Mouse Input" on page 162• "Redirect Storage Media" on page 162• "Add a New Server Session" on page 164• "Exit the Oracle ILOM Remote Console" on page 164
Secure the ILOM Remote Console	<ul style="list-style-type: none">• "Edit the ILOM Remote Console Lock Option" on page 165

Related Topics

For ILOM	Chapter or Section	In this guide
<ul style="list-style-type: none">• Concepts	<ul style="list-style-type: none">• Remote Host Management Options	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none">• CLI	<ul style="list-style-type: none">• Managing Remote Hosts Storage Redirection and Securing the ILOM Remote Console	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>

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

Managing Remote Hosts

ILOM provides different options for remotely managing hosts, for more information about these options consult the following table:

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• “Before You Begin” on page 153	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP• CMM
Oracle ILOM Remote Console	<ul style="list-style-type: none">• “Performing the Initial Setup Tasks to Enable ILOM Remote Console Video Redirection” on page 154• “Launching Redirection Using the Oracle ILOM Remote Console” on page 157	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP (enable KVMS state only)• CMM

Note – For information about the Remote Host Storage Redirection Command-Line Interface (CLI), see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Before You Begin

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

- You must use an Admin (a) or Console (c) role account to use the Oracle ILOM Remote Console.
- The Oracle ILOM Remote Console supports two methods of redirection: video and serial console. Video redirection is supported on all Oracle Sun x86 processor-based servers, as well as some SPARC processor-based servers. Serial console redirection is supported on all SPARC servers but it is currently not supported on x86 servers.
- To run the Oracle ILOM Remote Console, you must have the JRE 1.5 or higher (Java 5.0 or higher) software installed on your local client. To download the Java 1.5 runtime environment, go to: <http://java.com>.
- The Oracle ILOM Remote Console is supported on your local client with the operating systems, web browsers, and JVM listed in the following table:

Operating System	Web Browser	Java Virtual Machine (JVM)
Oracle Solaris (9 and 10)	<ul style="list-style-type: none">• Mozilla 1.7.5 and above• Firefox 1.0 and above	<ul style="list-style-type: none">• 32-bit JDK
Linux (Red Hat, SUSE, Ubuntu, Oracle)	<ul style="list-style-type: none">• Mozilla 1.7.5 and above• Firefox 1.0 and above• Opera 6.x and above	<ul style="list-style-type: none">• 32-bit JDK
Microsoft Windows (98, 2000, XP, Vista, and Windows 7)	<ul style="list-style-type: none">• Internet Explorer 6.0 and above• Mozilla 1.7.5 and above• Firefox 1.0 and above• Opera 6.x and above	<ul style="list-style-type: none">• 32-bit JDK

Performing the Initial Setup Tasks to Enable ILOM Remote Console Video Redirection

Topics

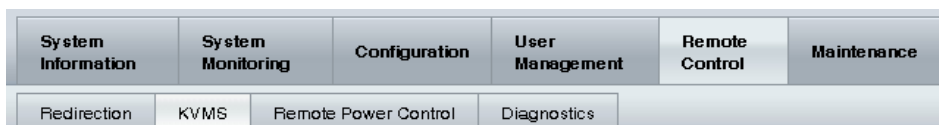
Description	Links	Platform Feature Support
Configure video redirection settings	<ul style="list-style-type: none">• “Configure ILOM Remote Control Video Redirection Settings” on page 154	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP (enable KVMS state only)
Register 32-bit JDK file prior to launching the ILOM Remote Console (for the first time) using Windows Internet Explorer	<ul style="list-style-type: none">• “Register 32-bit JDK File Type When Using Windows Internet Explorer” on page 156	<ul style="list-style-type: none">• x86 system server SP

Note – The initial setup procedures described in this section only apply to video redirection. If you are using only a serial console redirection, the initial setup tasks described in this section are not necessary. You can skip this initial setup section and proceed to [“Launching Redirection Using the Oracle ILOM Remote Console” on page 157](#).

▼ Configure ILOM Remote Control Video Redirection Settings

Follow these steps to configure ILOM settings for remote management of host servers:

1. **Log in to the ILOM SP web interface.**
2. **Click Remote Control --> KVMS.**
The KVMS Settings page appears.



KVMS Settings

Configure the state of the Keyboard, Video, Mouse and Storage (KVMS) service. Select a mode for your local mouse to use while managing the host remotely. Select Absolute mouse mode if your host is running Windows OS or Solaris, or Relative mouse mode for Linux OS. The Service Processor must be reset for any change in mouse mode to take effect.

State: Enabled

Mouse Mode:

Note – The Remote Control sub-tab options that are shown in the figure above differ depending on your Sun server. Likewise, the KVMS settings options on the KVMS Settings page differ depending on your Sun server. For more information, see the descriptions provided for the remote control settings in Step 3 of this procedure.

3. Use the options on the KVMS Settings page to specify the following remote control settings for managing a remote server.

Remote Control Setting	Applies To	Action
KVMS State	Video redirection	Check Enabled to enable the redirection of keyboard, video, mouse, and storage devices of the managed host. If left unchecked, the KVMS device redirection will be disabled.
Mouse Mode Settings	Video redirection	Select one of the following mouse mode settings: <ul style="list-style-type: none"> • Absolute. Select Absolute Mouse Mode for best performance when you are using Solaris or Windows operating systems. Absolute is the default. • Relative. Select Relative Mouse Mode when you are using a Linux operating system. Note that not all Linux operating systems support Absolute mode. <p>Note - As of ILOM 3.0.4 and later versions of ILOM, you can toggle between the relative and absolute settings without having restart the server SP. Changes take effect immediately in the ILOM Remote Console.</p>

▼ Register 32-bit JDK File Type When Using Windows Internet Explorer

If you will be using Windows Internet Explorer (IE) web browser to launch the ILOM Remote Console, you must register the 32-bit JDK file on your system before using IE to launch the Oracle ILOM Remote Console.

Follow these steps to register the 32-bit JDK file.

1. **On the Windows client, open Windows Explorer (not Internet Explorer).**
2. **In the Windows Explorer dialog, select `Tools --> Folder Options` then select the `Files Types` tab.**
3. **In the Files Types tab, do the following:**
 - a. **In the registered file type list, select the `JNLP` file type and click `Change`.**
 - b. **In the Open With... dialog, click `Browse` to select the 32-bit JDK file.**
 - c. **Select the checkbox for `Always use the selected program to open this kind of file`.**
 - d. **Click `OK`, then start the service for Storage Redirection in the ILOM web interface.**

Launching Redirection Using the Oracle ILOM Remote Console

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• “Before You Begin” on page 157	<ul style="list-style-type: none">• x86 system server SP
Launch redirection using Oracle ILOM Remote Console	<ul style="list-style-type: none">• “Launch the Oracle ILOM Remote Console” on page 158• “Start, Stop, or Restart Device Redirection” on page 160• “Redirect Keyboard Input” on page 160• “Control Keyboard Modes and Key Send Options” on page 161• “Redirect Mouse Input” on page 162• “Redirect Storage Media” on page 162• “Add a New Server Session” on page 164• “Exit the Oracle ILOM Remote Console” on page 164	<ul style="list-style-type: none">• SPARC system server SP• CMM

Before You Begin

The following requirements must be met prior to performing the remote management procedures in this section.

- You must have the Java Runtime Environment (1.5 or later) installed on your local system. To download the latest Java runtime environment, go to: <http://java.com>.
- The 32-bit JDK file needs to be specified when starting the ILOM Remote Console as described in the following procedure. However, if you are using Windows Internet Explorer to launch the ILOM Remote Console for the first time, you must first register the 32-bit JDK file on your system. For more details, see “Register 32-bit JDK File Type When Using Windows Internet Explorer” on page 156

- You must log in to the ILOM SP web interface using an Admin (a) or Console (c) role account. Either an Admin or Console role account is required to launch the Oracle ILOM Remote Console.
- You must have configured the Remote Control Settings in the ILOM web interface. For instructions, see ["Configure ILOM Remote Control Video Redirection Settings"](#) on page 154.

▼ Launch the Oracle ILOM Remote Console

1. Log in to the ILOM web interface for the server SP.
2. Click **Remote Control --> Redirection**.

The Launch Redirection page appears.

System Information		System Monitoring		Configuration		User Management		Remote Control		Maintenance			
Redirection		KVMs		Remote Power Control		Diagnostics		Host Control		Host Boot Mode		Keyswitch	

Launch Redirection

Manage the host remotely by redirecting the system console to your local machine. Launch the Sun ILOM Remote Console to utilize the RKVMS features. Select 16-bit high-quality color redirection for fast connections, or 8-bit lower-quality color redirection for slower connections. Select serial to access the Managed Host's serial console.

- I want to see redirection in 16-bit
- I want to see redirection in 8-bit
- I want to see serial redirection

[Launch Redirection](#)

Storage Redirection

You can optionally redirect local CDROM storage devices or CDROM image files from your workstation to the host by using the non-graphical storage redirection utility. This consists of a background service process running on your local machine that manages and maintains redirection to the host. This service is Java Web Start based and can be started by clicking 'Launch Service' below.

[Launch Service](#)

A scriptable, command-line Java client application is used to issue commands to the Service Processor for starting and stopping redirection of local storage devices and/or image files to one or more ILOM-enabled hosts. Click 'Download Client' below and save as StorageRedir.jar locally, and get started by running 'java -jar StorageRedir.jar -h' from a local command window prompt.

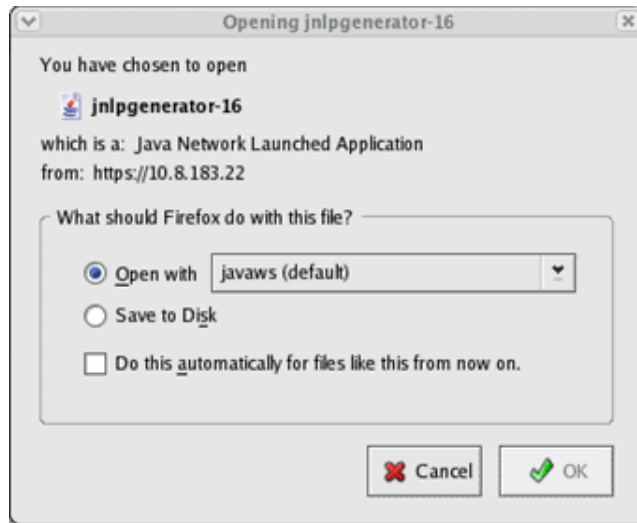
[Download Client](#)

Note – Depending on your platform, the Launch Redirection page will offer different combinations of redirection options. If multiple options are presented, select the type of redirection that you want to use to remotely manage this host.

3. To specify how you want to see the redirected system console, click one of the radio buttons.

4. Click Launch Redirection.

A dialog appears indicating the file type chosen to launch the program



5. In the Java Start Web Program dialog do the following:

a. Click Open with... to specify the 32-bit JDK file.

b. Select the check box for Do this automatically for files like this from now on.

Note – If a certificate warning message appears stating that the name of the site does not match the name on the certificate, click Run to continue.

The Oracle ILOM Remote Console window appears.

▼ Start, Stop, or Restart Device Redirection

1. In the Oracle ILOM Remote Console menu bar, click **Redirection**.
2. In the **Redirection** menu, specify, one of the following redirection options.

Option	Description
Start Redirection	Select Start Redirection to enable redirection of devices. Start Redirection is enabled by default.
Restart Redirection	Select Restart Redirection to stop and start redirection of devices. Typically, this option is used when a valid redirection is still established.
Stop Redirection	Select Stop Redirection to disable the redirection of devices

A confirmation message appears confirming that you want to change the redirection setting.

3. In the **Confirmation** message, click **Yes** to proceed or **No** to cancel the operation.

▼ Redirect Keyboard Input

Before You Begin

- This procedure only applies to serial console redirection.
- Although multiple users can connect to the system console, only one user at a time has write access to the console (that is, only one user can type commands into the system console). Any characters that other users type are ignored. This is referred to as a write lock, and the other user sessions are in read-only mode. If no other users are currently logged in to the system console, then you obtain the write lock automatically when you start keyboard redirection. If another user currently has write access to the console, you will be prompted to forcibly transfer write access away from their session.
- A server redirection session must be active for the remote host server SP. For details, see ["Add a New Server Session" on page 164](#).
- Device redirection must be started. For details, see ["Start, Stop, or Restart Device Redirection" on page 160](#).

Follow these steps to redirect a remote host server keyboard to your local client:

1. **Select Remote Control --> KVMS.**

The KVMS Settings page appears.

2. Select the KVMS Settings check box to enable the remote management state of the keyboard.

The KVMS State is enabled by default.

▼ Control Keyboard Modes and Key Send Options

Before You Begin

- A server redirection session must be active for the remote host server SP. For details, see ["Add a New Server Session" on page 164](#).
- Device redirection must be started. For details, ["Start, Stop, or Restart Device Redirection" on page 160](#)
- Keyboard redirection must be enabled. For details, see ["Redirect Keyboard Input" on page 160](#).

Follow these steps to control keyboard modes and individual key send options:

1. In the Oracle ILOM Remote Console window, click the Keyboard menu.
2. In the Keyboard menu, specify any of the following keyboard settings.

Option	Description
Auto-keybreak Mode	Select Auto-keybreak Mode to automatically send a keybreak after every key press. Use this option to help resolve keyboard problems over slow network connections. The Auto-keybreak Mode is enabled by default.
Stateful Key Locking	Select Stateful Key Locking if your client uses stateful key locking. Stateful Key Locking applies to these three lock keys: Caps Lock, Num Lock, and Scroll Lock.
Left Alt Key* *Not available on Windows Client	Select the Left Alt Key to toggle the left Alt Key on or off.
Right Alt Key* *Not available on Windows Client	Select Right Alt Key to toggle the right Alt Key on or off for non-US keyboards. When enabled, this option enables you to type the third key character on a key. This keyboard option provides the same capabilities of an Alt Graph key.
F10	Select F10 to apply the F10 function key (typically used in BIOS).

Control Alt Delete	Select Control Alt Delete to send the Control-Alt-Delete sequence.
Control Space	Select Control Space to send a Control-Space sequence to enable input on remote host.
Caps Lock	Select Caps Lock to send the Caps Lock key to enable input with Russian and Greek keyboards.

Note – Not all of these keyboard settings apply during serial redirection.

▼ Redirect Mouse Input

Before You Begin

- Mouse redirection is only supported for video redirection settings.
- Configure your mouse settings to Absolute or Relative Mouse Mode. See ["Configure ILOM Remote Control Video Redirection Settings" on page 154.](#)
- A server redirection session must be active for the remote host server SP. For details, see ["Add a New Server Session" on page 164.](#)
- Device redirection must be started. For details, ["Start, Stop, or Restart Device Redirection" on page 160.](#)

Follow these steps to redirect a remote host server mouse to your local client:

1. Select Remote Control --> KVMS.

The KVMS Settings page is displayed.

2. Select the KVMS State check box to enable the remote host management state of the mouse.

The KVMS State is set to Enabled by default.

▼ Redirect Storage Media

Before You Begin

- A server redirection session must be active for the remote host server SP. For details, see ["Add a New Server Session" on page 164.](#)
- Device redirection must be started. For details, ["Start, Stop, or Restart Device Redirection" on page 160](#)

- For Solaris client systems, you must perform the following actions prior to redirecting storage devices:
 - If Volume Manager is enabled, you will need to disable this feature.
 - Assign root privilege to the processor that is running the Oracle ILOM Remote Console by entering these commands:

```
su to root
```

```
ppriv -s +file_dac_read pid_javarconsole
```

Follow these steps to redirect storage media (CD/DVD or ISO image) from your desktop to a host server:

1. In the Oracle ILOM Remote Console menu bar, select Devices.

2. In the Devices menu, perform the following actions:

a. Enable the appropriate storage device or image setting.

Option	Description
CD-ROM	Select CD-ROM to enable the local CD device. This option causes your local CD-ROM drive to behave as though it were a CD device directly attached to the remote host server.
Floppy	Select Floppy to enable the local floppy device. This option causes your local floppy drive to behave as though it were a floppy device directly attached to the remote host server.
CD-ROM Image	Select CD-ROM Image to specify the location of a CD-ROM image on your local client or network share.
Floppy Image	Select Floppy Image to specify the location of a floppy image on your local client or network share.

Note – Floppy storage media redirection is not supported on SPARC systems.

Note – If you are installing software from distribution media (CD/DVD), ensure that the media is inserted in the redirected drive. If you are installing software from an ISO image, ensure that the ISO image is stored on your local client or network shared file system.

A dialog appears prompting you to specify a storage drive location or image file location.

b. To specify the storage drive location or image file location, perform one of the following actions:

- In the Drive Selection dialog, select or type a drive location, then click OK.

- In the File Open dialog, browse to the location of the image, then click OK.
3. **To reuse these storage settings on the host at a later time, click Devices --> Save as Host Default.**

▼ Add a New Server Session

1. **In the Oracle ILOM Remote Console window, select Redirection --> New Session.**

The New Session Creation dialog appears.

2. **In the New Session Creation dialog, type the IP address of a remote host server SP, then click OK.**

The Login dialog appears.

3. **In the Login dialog, type a user name and password.**

A session tab for the newly added remote host server appears in the tab set of the Oracle ILOM Remote Console.

Note – The Login dialog will also ask you whether the new session is to be video redirection (which is supported on all x64 systems and some SPARC systems) or serial redirection (which is currently supported on SPARC systems). Consult your platform documentation for more information about which type of redirection is supported.

▼ Exit the Oracle ILOM Remote Console

Follow this step to exit the Oracle ILOM Remote Console and close all remote server sessions:

- **In the Oracle ILOM Remote Console menu bar, select Redirection --> Quit.**

Securing the ILOM Remote Console

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• “Before You Begin” on page 165	<ul style="list-style-type: none">• x86 system server SP
Edit the ILOM Remote Console lock settings	<ul style="list-style-type: none">• “Edit the ILOM Remote Console Lock Option” on page 165	<ul style="list-style-type: none">• SPARC system server SP• CMM

Before You Begin

- To enable the ILOM Remote Console Lock option in ILOM, you must have Console (c) role privileges associated with your user account.
- You must be running ILOM 3.0.4 or later on the server SP.

▼ Edit the ILOM Remote Console Lock Option

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

Note – When logging in to the CMM web interface, navigate to the SP target where you want to enable or disable the KVMS lock option for the ILOM Remote Console.

2. **In the web interface page, click Remote Console --> KVMS.**

The KVMS page appears displaying the options available for KVMS Settings and Host Lock Settings.

3. **In the Host Lock Settings section of the KVMS page, perform one of the following tasks:**

Task	Instructions
Enable the standard Windows host lock mode option.	<ul style="list-style-type: none"> • In the Lock Mode list box, select Windows.
Enable the custom host lock mode feature.	<ol style="list-style-type: none"> 1. In the Lock Mode list box, select Custom. 2. In the Custom Lock Modifiers list box, select up to four custom modifiers that match the keyboard shortcut modifiers that are predefined in your operating system. 3. In the Custom Lock Key list box, select the key that matches the keyboard shortcut key that is predefined in your operating system.
Disable the host lock mode feature.	<ul style="list-style-type: none"> • In the Lock Mode list box, select Disabled.

4. Click Save to apply the changes you specified.

Managing Remote Hosts Power States

Topics

Description	Links
Control the power state of a remote server module or CMM	<ul style="list-style-type: none"> • “Controlling Power States on Remote Server SP or CMM” on page 168
Control x86 Host boot device settings	<ul style="list-style-type: none"> • “Managing Host Control of BIOS Boot Device on x86 Systems” on page 169

Related Topics

For ILOM	Chapter or Section	In this guide
<ul style="list-style-type: none"> • Concepts 	<ul style="list-style-type: none"> • Remote Host Management Options 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none"> • CLI 	<ul style="list-style-type: none"> • Managing Remote Hosts Power States 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Controlling Power States on Remote Server SP or CMM

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• “Before You Begin” on page 168	<ul style="list-style-type: none">• x86 system server SP• SPARC system server SP
Control the power state of the remote host server	<ul style="list-style-type: none">• “Control Power State of Remote Host Server Using Server SP Web” on page 168• “Control Power State of Remote Chassis Using the CMM Web Interface” on page 169	<ul style="list-style-type: none">• CMM

Before You Begin

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

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

1. **Log in to the 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

1. Log in to the CMM ILOM 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 OSs 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 BIOS Boot Device on x86 Systems

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none"> • “Before You Begin” on page 170 	<ul style="list-style-type: none"> • x86 system server SP
Override host boot device order in BIOS	<ul style="list-style-type: none"> • “Configure BIOS Host Boot Device Override” on page 170 	

Before You Begin

- The Reset and Host Control (r) role is required to change the host boot device configuration variable.
- The Host Control -BIOS boot device feature is supported on x86 system SPs. This feature is not supported on the CMM or on SPARC system SPs. For information about ILOM Host Control boot options on SPARC systems, consult the online ILOM Supplement guide or Platform Administration guide published for that system.

Follow the steps in the following procedure to override the BIOS boot device setting from ILOM by using the Host Control features.

▼ Configure BIOS Host Boot Device Override

1. Log in to ILOM SP web interface.

2. Click **Remote Control** --> **Host Control**.

The Host Control page appears.

System Information	System Monitoring	Configuration	User Management	Remote Control	Maintenance
Redirection	KVMS	Remote Power Control	Diagnostics	Host Control	

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:

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. Click Save for your changes to take effect.

Managing TPM and LDom States on SPARC Servers

Topics

Description	Links
Control the TPM state on a SPARC server	<ul style="list-style-type: none"> • “Controlling the TPM State on SPARC Servers” on page 174
Manage Logical Domain (LDom) configurations on SPARC servers	<ul style="list-style-type: none"> • “Managing LDom Configurations on SPARC Servers” on page 175

Related Topics

For ILOM	Chapter or Section	In this guide
<ul style="list-style-type: none"> • Concepts 	<ul style="list-style-type: none"> • Remote Host Management Options 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none"> • CLI 	<ul style="list-style-type: none"> • Managing TPM and LDom States on SPARC Servers 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Controlling the TPM State on SPARC Servers

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• “Before You Begin” on page 174	<ul style="list-style-type: none">• SPARC system SP
Control the TPM state on a SPARC server.	<ul style="list-style-type: none">• “Control TPM State on a SPARC Server” on page 174	

Before You Begin

- The TPM feature in 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 Solaris, see the Solaris documentation or the platform documentation shipped with your server.

- You must be using ILOM 3.0.8 or a later version on the SPARC server SP.
- You need to have the Reset and Host Control (r) user account to modify the TPM settings in ILOM.

▼ Control TPM State on a SPARC Server

1. **Log in to the ILOM SP 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** – Select the `Enable True` check box to enable the TPM state on the SPARC server.

- **Activate** – Select `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** – Select the `Enable True` check box to disable the TPM state on the SPARC.
 - **Activate** – Select the `Activate True` check box to activate the configuration change on the SPARC server.
 - **Forceclear** – Select `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

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none"> • “Before You Begin” on page 176 	<ul style="list-style-type: none"> • SPARC system SP
View and manage ILOM settings for stored LDom configurations.	<ul style="list-style-type: none"> • “View Stored LDom Configurations on SPARC T3 Series Server” on page 176 • “Configure Host Power to Stored LDom Configurations” on page 177 • “Specify Host Power to a Stored LDom Configuration” on page 178 	

Before You Begin

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

- You must access ILOM on a SPARC server that has the appropriate ILOM point release firmware installed (see Note below).

Note – ILOM 3.0.12 or later is required to view the LDom targets and properties from a SPARC T3 Series server. ILOM 2.0.0 or later is required to: (1) specify which LDom configuration is used on the host SPARC server, and (2) to manage the boot property values for the control domain from the host SPARC server.

- You must have the Oracle VM Server for SPARC (Logical Domains Manager) 2.0 or later software installed on your host SPARC server.
- The host SPARC server must have saved LDom configurations. For instructions on how to create and save LDom configurations on a host SPARC server, see the *Logical Domains 1.3 Administration Guide* (821-0406).
- You must have Remote Host Reset and Host Control (x) privileges in ILOM to set the:
 - LDom bootmode target
 - Bootmode property values for the primary or guests domain

▼ View Stored LDom Configurations on SPARC T3 Series Server

1. **Log in to the 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.**

Redirection KVMS Remote Power Control Diagnostics Host Control Host Boot Mode Host Domain Keyswitch TPM

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
LDMCONFIG0	1970-01-01 00:00:01	3
LDMCONFIG1	1970-01-01 00:01:05	6
LDMCONFIG2	1970-01-01 00:02:09	9
LDMCONFIG3	1970-01-01 00:03:13	12
LDMCONFIG4	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

1. Log in to the 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 checkboxes.

By default, the Auto Boot checkbox 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

1. Log in to the 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:

Expiration Date: Tue Jan 19 03:14:07 2038

Script:

LDOM Config:

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	<p>In the State list box, select one of the following options:</p> <ul style="list-style-type: none">• 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. <p>The State dictates the boot mode at reset.</p> <p>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.</p>
Script	<p>Specify a boot script.</p> <p>The script controls the host server OpenBoot PROM firmware method of booting. It does not affect the current <code>/HOST/bootmode</code> setting.</p>
LDOM Config	<p>Specify a saved LDom configuration file name.</p>

4. To commit the changes made on the Host Boot Mode Settings page, click Save.

Performing Remote Host System Diagnostics

Topics

Description	Links
Diagnose x64 system hardware issues	<ul style="list-style-type: none"> • “Diagnosing x86 Systems Hardware Issues” on page 180
Diagnose SPARC system hardware issues	<ul style="list-style-type: none"> • “Diagnosing SPARC Systems Hardware Issues” on page 182
Collect data for use by Oracle Services personnel to diagnose system problems	<ul style="list-style-type: none"> • “Collecting SP Data to Diagnose System Problems” on page 183

Related Topics

For ILOM	Chapter or Section	In this guide
<ul style="list-style-type: none"> • Concepts 	<ul style="list-style-type: none"> • Diagnostics for x86 or SPARC Systems • Collect SP Data to Diagnose System Problems 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide (820-6410)</i>
<ul style="list-style-type: none"> • CLI 	<ul style="list-style-type: none"> • Diagnostics • Collect SP Data to Diagnose System Problems 	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412)</i>

The ILOM 3.0 Documentation Collection is available at:

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

Diagnosing x86 Systems Hardware Issues

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• “Before You Begin” on page 180	<ul style="list-style-type: none">• x86 system server SP
Diagnose x86 system hardware issues	<ul style="list-style-type: none">• “Configure Pc-Check Diagnostics for x86 Systems” on page 180• “Generate a NMI” on page 181	

Note – For additional information about common x86 diagnostic tools, see *Oracle x86 Servers Diagnostic Guide* (820-6750).

Before You Begin

- To diagnose x86 systems hardware issues, you need the Reset and Host Control (r) role enabled.

▼ Configure Pc-Check Diagnostics for x86 Systems

Note – After you configure the Pc-Check Diagnostics, you must reset the host to run diagnostic tests.

Follow these steps to configure Pc-Check diagnostics:

1. **Log in to the ILOM SP web interface.**
2. **Click Remote Control --> Diagnostics.**
The Diagnostics page appears.
3. **From the Run Diagnostics on Boot drop-down list, select one of the following options:**

- **Disabled** – Select Disabled if you do not want to run Pc-Check diagnostic tests upon startup of a remote host server.
- **Enabled** – Select Enabled if you want to run basic Pc-Check diagnostic tests upon start-up of the remote host server. These basic diagnostic tests typically take 5 minutes to complete.
- **Extended** – Select Extended if you want to run extended Pc-Check diagnostic tests upon start-up of the remote host server. These extended diagnostic tests typically take 20 to 40 minutes to complete.
- **Manual** – Select Manual if you want to run select Pc-Check diagnostic tests upon start-up of the remote host server.

4. Click Save for your settings to take effect.

If you selected the Manual option, the graphical interface for Pc-Check Diagnostics appears after the host is reset. From this interface, you can select which Pc-Check diagnostic tests to run.

▼ Generate a NMI



Caution – Depending on the host operating system configuration, generating a non-maskable interrupt (NMI) might cause the operating system to crash, stop responding, or wait for external debugger input.

Follow these steps to generate a NMI:

- 1. Log in to the ILOM SP web interface.**
- 2. Click Remote Control --> Diagnostics.**
The Diagnostics page appears.
- 3. Click the Generate NMI button.**

A non-maskable interrupt (NMI) is generated to the host operating system.

Diagnosing SPARC Systems Hardware Issues

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none">• “Before You Begin” on page 182	<ul style="list-style-type: none">• SPARC system server SP
Diagnose SPARC system hardware issues	<ul style="list-style-type: none">• “Configure Diagnostics Settings for SPARC Systems” on page 182	

Before You Begin

- To configure and run diagnostic tests on a SPARC processor-based system, you need the Reset and Host control (r) role enabled.

▼ Configure Diagnostics Settings for SPARC Systems

Follow these steps to configure diagnostic settings for SPARC systems:

1. **Log in to the ILOM SP web interface.**
2. **Click Remote Control --> Diagnostics.**
The Diagnostics page appears.
3. **Select a value for Trigger:**
 - **Power On** – Diagnostics will be run when power is applied.
 - **User Reset** – Diagnostics will be run upon a user-invoked reset.
 - **Error Reset** – Diagnostics will be run upon any error-invoked reset.
4. **Select a value for Verbosity for each trigger type:**
 - **None** – Diagnostics do not print any output on the system console when running, unless a fault is detected.

- **Min** – Diagnostics print a limited amount of output on the system console (the default value).
 - **Normal** – Diagnostics print a moderate amount of output on the system console, including the name and results of each test being run.
 - **Debug** – Diagnostics print extensive debugging output on the system console, including devices being tested and debug output of each test.
5. **Select a value for Level for each trigger type:**
- **Min** – Run the minimum level of diagnostics to verify the system.
 - **Max** – Run the maximum set of diagnostics to fully verify system health (the default value).
6. **Select a value for Mode:**
- **Off** – Do not run any diagnostics.
 - **Normal** – Run diagnostics (the default value).
7. **Click Save for your settings to take effect.**

Collecting SP Data to Diagnose System Problems

Topics

Description	Links	Platform Feature Support
Review the prerequisites	<ul style="list-style-type: none"> • “Before You Begin” on page 183 	<ul style="list-style-type: none"> • Oracle Service personnel feature only
Collect SP data	<ul style="list-style-type: none"> • “Collect SP Data to Diagnose System Problems” on page 184 	

Before You Begin

- To collect SP data using the Service Snapshot utility, you need the Admin (a) role enabled.

Follow the steps in the following procedure to override the BIOS boot device setting from ILOM by using the Host Control features.



Caution – The purpose of the ILOM Service Snapshot utility is to collect data for use by Oracle Services personnel to diagnose system problems. Customers should not run this utility unless requested to do so by Oracle Services.

▼ Collect SP Data to Diagnose System Problems

1. Log in to the ILOM SP web interface.

2. Click **Maintenance** --> **Snapshot**.

The Service Snapshot Utility page appears.

The screenshot shows the 'Service Snapshot Utility' page in the ILOM web interface. At the top, there is a navigation bar with tabs for 'System Information', 'System Monitoring', 'Configuration', 'User Management', 'Remote Control', and 'Maintenance'. Below this, there is a sub-menu with 'Firmware Upgrade', 'Backup/Restore', 'Reset SP', 'Configuration Management', and 'Snapshot'. The main content area is titled 'Service Snapshot Utility' and contains the following elements:

- A 'Data Set' dropdown menu set to 'Normal'.
- Two checkboxes: 'Collect Only Log Files From Data Set' (unchecked) and 'Encrypt Output File' (unchecked).
- A 'Transfer Output File' section with a 'Transfer Method' dropdown set to 'Browser' and a note: 'The downloaded file will be saved according to your browser settings.'
- A blue 'Run' button.

3. Select the desired **Data Set**: **Normal**, **FRUID**, **Full**, or **Custom**.

- **Normal** – Specifies that ILOM, operating system, and hardware information is collected.
- **FRUID** – Available as of ILOM 3.0.3, specifies that information about FRUs currently configured on your server in addition to the data collected by the Normal set option is collected.
- **Full** – Specifies that all data is to be collected. Selecting Full might reset the system.
- **Custom** – Allows you to choose one or more of the following data sets:

- ILOM Data
 - Hardware Data
 - Basic OS Data
 - Diagnostic Data
 - FRUID data
4. **Click the Enabled check box if you want to collect only log files from the data set.**
 5. **Click the Enabled check box if you want to encrypt the output file.**
 6. **Select one of the following methods to transfer the output file:**
 - Browser
 - SFTP
 - FTP
 7. **Click Run.**

A Save As dialog box appears.
 8. **In the dialog box, specify the directory to which to save the file and the file name.**
 9. **Click OK.**

The file is saved to the specified directory.

Diagnosing IPv4 or IPv6 ILOM Connection Issues

If you are experiencing difficulties with connecting to ILOM when using IPv6, see [TABLE A-1](#) to help resolve common problems when accessing ILOM using IPv6.

TABLE A-1 Common IPv6 Connection Problems and Suggested Resolutions

IPv6 Common Connection Problems	Suggested Resolution
Unable to access the ILOM web interface using an IPv6 address.	Ensure that the IPv6 address in the URL is enclosed by brackets, for example: <code>https://[fe80::221:28ff:fe77:1402]</code>
Unable to download a file using an IPv6 address.	Ensure that the IPv6 address in the URL is enabled by brackets, for example: <code>load -source tftp://[fec0:a:8:b7:214:rfff:fe01:851d]desktop.pkg</code>
Unable to access ILOM using IPv6 from a network client.	<p>If on a separate subnet, try the following:</p> <ul style="list-style-type: none"> • Verify that ILOM has a dynamic or static address (not just a Link-Local address). • Verify that the network client has IPv6 address configured (not just a Link-Local address). <p>If on the same or separate subnet, try the following</p> <ul style="list-style-type: none"> • Ensure that setting for <code>IPv6 State</code> is enabled on the Network Settings Page in the ILOM web interface or under the <code>/SP/network/ipv6</code> target in the ILOM CLI. • Run <code>ping6</code> in a restricted shell. • Run <code>tracert</code> in a restricted shell.

TABLE A-1 Common IPv6 Connection Problems and Suggested Resolutions (*Continued*)

IPv6 Common Connection Problems	Suggested Resolution
Unable to access ILOM from a client within a dual-stack IPv4 and IPv6 network environment.	Ensure that the following settings are enabled: <ul style="list-style-type: none">• <i>State</i>. You can enable the setting for <i>State</i> on the Network Settings page in the ILOM web interface or under the <code>/SP/network</code> target in the CLI.• <i>IPv6 State</i>. You can enable the setting for <i>IPv6 State</i> on the Network Settings page in the ILOM web interface or under the <code>/SP/network/ipv6</code> target.
Unable to access ILOM using IPv4 from a network client.	Ensure that the setting for <i>State</i> is enabled on the Network Settings page in the ILOM web interface or under the <code>/SP/network</code> target in the ILOM CLI.

Manual Host OS Configuration Guidelines for Local Interconnect Interface

If you chose to manually configure a non-routable IPv4 address for the ILOM SP connection point on the Local Interconnect Interface, you will also need to manually configure a non-routable IPv4 address for the host OS connection point on the Local Interconnect Interface. General guidelines, per operating system, for configuring a static non-routable IPv4 address for the host OS connection point are provided below. For additional information about configuring IP addresses on the host operating system, consult the vendor operating system documentation.

Note – ILOM will present the internal USB Ethernet device installed on your server as an USB Ethernet interface to the host operating system.

TABLE B-1 General Guidelines for Configuring Internal USB Ethernet Device on Host OS

Operating System	General Guidelines
Windows Server 2008	<p>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 <i>Oracle Server Hardware Management Pack User's Guide</i> (821-1609).</p> <p>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).</p> <p>For more information about configuring an IPv4 address in Windows 2008, see the Microsoft Windows Operating System documentation or the Microsoft Tech Net site (http://technet.microsoft.com/en-us/library/cc754203%28WS.10%29.aspx).</p>
Linux	<p>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.</p> <p>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:</p> <pre data-bbox="348 1097 958 1286">\>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</pre> <p>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.</p> <p>For more information about how to configure an IP address for device using a Linux operation system, see the Linux operating system documentation.</p>

TABLE B-1 General Guidelines for Configuring Internal USB Ethernet Device on Host OS (*Continued*)

Operating System	General Guidelines
Solaris	<p>Most Solaris Operating System installations on a Oracle Sun platform server include the installation of the device driver for an internal USB Ethernet device. If this driver was not supported, you can extract this driver from the Oracle Hardware Management Pack 2.1.0 or later software. For information about how to extract the Solaris-specific OS driver for the Ethernet interface, see the <i>Oracle Server Hardware Management Pack User's Guide</i> (821-1609).</p> <p>Typically, the internal USB Ethernet device is automatically discovered by the Solaris operating system. The internal Ethernet device typically appears as <code>usbem0</code>. However, the name for the internal Ethernet device might be different based on the distribution of the Solaris operating system.</p> <p>After the Solaris Operating System recognizes the local USB Ethernet device, the IP interface for the USB Ethernet device needs to be configured.</p> <p>The following instructions demonstrate how to configure a static IP address corresponding to <code>usbem0</code>, which typically represents an internal USB Ethernet device found on the server.</p> <ul style="list-style-type: none">• Type the following command to <code>plumb</code> the IP interface or <code>unplumb</code> the IP interface: <code>ifconfig usbem0 plumb</code> <code>ifconfig usbem0 unplumb</code>• Type the following commands to set the address information: <code>ifconfig usbem0 netmask 255.255.255.0 broadcast 169.254.182.255 169.254.182.77</code>• To set up the interface, type: <code>ifconfig usbem0 up</code>• To bring the interface down, type: <code>ifconfig usbem0 down</code>• To show the active interfaces, type: <code>ifconfig -a</code>• To test connectivity, ping the Solaris host or the SP internal USB Ethernet device. <code>ping <IPv4 address of Solaris Host></code> <code>ping <IPv4 address of SP-Ethernet USB></code> <p>Note - Rather than performing the typical <code>ifconfig</code> steps, it is possible to script the configuration of the interface. However, the exact network scripts can vary among the Solaris distributions. Typically, the operating version will have examples to model the network scripts.</p> <p>For more information about how to configure a static IP address for a device using the Solaris Operating System, see the Solaris Operating System documentation.</p>

Note – If the internal USB Ethernet device driver was not included in your operating system installation, you can obtain the device driver for the Ethernet device from the Oracle Hardware Management Pack 2.1.0 or later software. For more information about extracting this file from the Management Pack, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609).

Index

A

Active Directory

- certificate, 56
- certificate file upload, 56
- configuring, 52
- event class, 61
 - event class custom filter, 61
- loading certificate, 56
- removing certificate, 56
- strict certificate mode, 56
- tables, 57
 - Admin Groups, 57
 - Alternate Servers, 59
 - Custom Groups, 58
 - DNS Locator Queries, 60
 - Operator Groups, 58
 - User Domains, 58
- troubleshooting, 60

Administrator role, 47

alert rules

- creating or editing, 99
- disabling, 100
- generating tests, 100

alerts

- generating email notification, 102
- generating test alerts, 100

automatic IP address, 25

B

back up and restore, 133

back up XML file, 139

Backup operation

- passphrase, if not used, 136
- sensitive data requirements, 136
- suggested user account roles, 134
- supported transfer methods, 135
- using the web interface, 134

backup XML file

- editing, adding a user account, 141
- editing, example of, 140
- editing, passwords, 141
- editing, roles, 141

baud rate

- setting, 34

browser and software requirements, 2

C

chassis monitoring module (CMM), configuring IP

- addresses
- editing through an Ethernet connection, 36

clock settings

- configuring, 82

components

- changing information, 76
- enabling and disabling, 78
- event log, 80
- indicators, 80
- managing, 76
- monitoring, 79
- preparing to remove, 78
- returning to service, 78
- sensors, 80
- viewing information, 76

configuration

- backing up, 133

- restoring, 133
- create or edit alert rules, 99

D

- diagnostics, 179
- Distinguished Name (DN) format, 58
- documentation, xiii
- Domain Name Service (DNS)
 - viewing and configuring, 32

E

- event log
 - custom filters, 71
 - filtering output, 83
 - viewing and clearing, 85

F

- firmware
 - downloading on x64 systems, 147
 - identifying version, 147
 - troubleshoot update session, 149
 - troubleshooting update session, 149
 - updating image, 148
 - upgrading, 148
 - verification, 148

H

- host name
 - assigning, 31
- host power state
 - controlling, 167, 168
- HTTP or HTTPS web access
 - enabling, 35 to 36

I

- ILOM configuration
 - resetting, 142
 - restoring, 136
- ILOM version numbers, xv
- IP address
 - assigning or changing, 36

K

- key send options, 161
- keyboard modes, 161
- Keyboard/Video/Mouse/Screen (KVMS), 154

- KVMS, 154

L

- LDAP
 - configuring ILOM for LDAP, 63
 - configuring the LDAP server, 62
 - object classes, 62
- LDAP/SSL
 - admin groups, 69
 - alternate servers, 69
 - certificate file upload, 67
 - configure, 64
 - custom groups, 69
 - event class, 72
 - operator groups, 69
 - tables, 68
 - Admin Groups, 69
 - Alternative Servers, 70
 - Custom Groups, 70
 - Operator Groups, 69
 - User Domains, 70
 - troubleshooting authentication and authorization, 71
 - user domains, 69
 - web interface tables, 68
- load certificate, 68
- Location, 32
- logging in to ILOM, 15
- logging out of ILOM, 19
 - using the web interface, 19

N

- navigation tabs, 9
- network settings
 - configuring, 23
 - pending and active properties, 24
 - viewing and configuring, 25
- non-maskable interrupt (NMI)
 - generating, 181

O

- Operator role, 47

P

- Pc-Check diagnostics, 180
- port ID, 60
- power consumption

- monitoring, 109
- monitoring individual power supply, 111
- monitoring system, 110

profile

- choosing, 46

R

RADIUS

- configuring, 73

redirect keyboard and mouse, 160

redirection

- keyboard input, 160
- mouse input, 162
- remote console video, 154
- start, stop, restart, 160
- storage media, 162

Remote Console

- configuration for remote control, 154
- exiting session, 164
- keyboard control modes, 161
- launching, 157
- new server session, 164
- redirecting keyboard and mouse, 160
- redirecting storage device or ISO image, 163 to 164
- serial redirection, 160
- video redirection, 154

remote diagnostic configuration

- SPARC systems, 182
- x64 systems, 180

remote hosts

- managing, 151
- managing power states, 167

remote syslog, 86

remove certificate, 68

resetting ILOM configuration, 150

Restore operation

- passphrase requirements, 138
- sessions momentarily suspended, 138
- suggested user roles, 137
- supported transfer methods, 137

restoring ILOM configuration, 136

roles

- Admin (a), 46
- Advanced, 46
- Console (c), 46
- Read Only (o), 46

Reset and Host Control (r), 46

Service (s), 46

User Management (u), 46

S

Secure Shell (SSH) settings

- configuring, 37
- enabling or disabling, 38
- generating new key, 38
- restarting the server, 38

Secure Socket Layer (SSL) certificate

- uploading certificate, 37

sensor readings, 80

serial port output

- switch using ILOM web interface, 34

serial port, internal

- setting baud rate, 34

Service Processor (SP)

- collecting and diagnosing, 184
- resetting, 150

Service Snapshot utility, 184

- data set, 184

session time-out

- resetting, 45
- setting, 45

single sign on

- configuring, 45

SMTP client, 101

- enabling, 102

SPARC servers

- managing TPM and LDom states, 173

SSH key, 38

- adding, 49
- configuring, 49
- deleting, 51
- supported transfer methods, 50
 - browser, 50
 - FTP, 50
 - HTTP, 50
 - HTTPS, 50
 - SCP, 50
 - SFTP, 50
 - TFTP, 50

static IP address, 26

storage components

- monitoring, 89

system contact field, 32

- system identifier
 - assigning, 31
- system identifier field, 32
- system indicators, 81
- system location field, 32

T

- timezone settings
 - configuring, 83
 - viewing or setting, 83

U

- user account
 - adding, 45
 - assigning roles, 45
 - configuring, 47
 - deleting, 48
- user profile
 - modifying, 47
- user sessions
 - viewing, 48

V

- video redirection, 154

W

- web interface
 - buttons, 5
 - components, 5
 - overview, 1, 2
 - supported browsers, 2

X

- XML file
 - backing up, 139