

Oracle Integrated Lights Out Manager (ILOM) 3.0

Daily Management — Concepts Guide



Part No.: E21447-03
September 2013

Copyright © 2010, 2013, 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 © 2010, 2013, 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.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.



Adobe PostScript

Contents

Using This Documentation ix

- ▼ Download Product Software and Firmware xi

Oracle ILOM Overview 1

- What Is Oracle ILOM? 2
- What Does Oracle ILOM Do? 2
- Oracle ILOM Features and Functionality 4
- New Features in Oracle ILOM 3.0 5
- User Accounts – Backward Compatibility 6
- Preconfigured User Accounts 7
 - root User Account 7
 - root Factory Default Password Warning Message 7
 - default User Account 8
- Oracle ILOM Supported Interfaces 9
- Oracle ILOM on the Server SP and CMM 10
- System Banner Messages 10

Network Configurations 13

- Oracle ILOM Network Management 14
 - Oracle ILOM Connection Methods 14
 - Initial Setup Worksheet 15
 - Default Network Port Used By Oracle ILOM 16
- Switch Serial Port Console Output (Serial Port Owner) 18

Oracle ILOM Communication Settings	18
SP Management Port – Recommended Practice for Spanning Tree Parameters	19
Network Configurations for IPv4	19
Dual-Stack Network Configurations for IPv4 and IPv6 (ILOM 3.0.12)	20
Oracle ILOM IPv6 Enhancements	21
Dual-Stack Network Options in Oracle ILOM CLI and Web Interface	23
Legacy Sun Server Platforms Not Supporting IPv6	24
Local Interconnect Interface: Local Connection to ILOM From Host OS	24
Platform Server Support and Oracle ILOM Access Through the Local Interconnect Interface	25
Local Interconnect Interface Configuration Options	26
Local Host Interconnect Configuration Settings in Oracle ILOM	27
User Account Management	31
Guidelines for Managing User Accounts	31
User Account Roles and Privileges	32
Oracle ILOM 3.0 User Account Roles	32
Single Sign On	33
SSH User Key-Based Authentication	34
Active Directory	34
User Authentication and Authorization	35
User Authorization Levels	35
Lightweight Directory Access Protocol	36
LDAP/SSL	36
RADIUS	37
System Monitoring and Alert Management	39
System Monitoring	40

Sensor Readings	41
System Indicators	41
Supported System Indicator States	41
Types of System Indicator States	42
Component Management	42
Fault Management	45
Clear Faults After Replacement of Faulted Components on Server or CMM	46
Oracle ILOM Event Log	47
Event Log Time Stamps and Oracle ILOM Clock Settings	48
Manage Event Log and Time Stamps From CLI, Web, or SNMP Host	48
Syslog Information	48
Collect SP Data to Diagnose System Problems	49
Alert Management	49
Alert Rule Configuration	49
Alert Rule Property Definitions	50
Alert Management From the CLI	53
Alert Management From the Web Interface	54
Alert Management From an SNMP Host	54
Storage Monitoring and Zone Management	57
Storage Monitoring for HDDs and RAID Controllers	57
CLI Storage Properties Shown for HDDs and RAID Controllers	58
RAID Status Definitions for Physical and Logical Drives	60
Monitoring Storage Components Using the CLI	61
Monitoring Storage Components Using the Web Interface	61
RAID Controllers Tab Details	62
Disks Attached to RAID Controllers Details	63
RAID Controller Volume Details	65

CMM Zone Management Feature 66

Power Monitoring and Management of Hardware Interfaces 67

Summary of Power Management Feature Updates 68

Power Monitoring Terminology 70

Real-Time Power Monitoring and Management Features 73

System Power Consumption Metrics 73

Web Interface Power Consumption Metrics as of Oracle ILOM 3.0 74

CLI Power Consumption Metrics as of Oracle ILOM 3.0 75

Web Interface Server and CMM Power Consumption Metrics As of
Oracle ILOM 3.0.4 76

Web Enhancements for Server SP Power Consumption Metrics As of
3.0.8 77

Web Enhancements for CMM Power Consumption Metrics As of
3.0.10 78

Power Policy Settings for Managing Server Power Usage 80

Power Policy Settings as of Oracle ILOM 3.0 80

Power Policy Settings as of Oracle ILOM 3.0.4 81

Power Capping Policy Settings as of Oracle ILOM 3.0.8 81

Power Usage Statistics and History Metrics for Server SP and CMM 83

Web Interface Power Usage Statistics and History Metrics 84

Power Usage Statistics and History as of Oracle ILOM 3.0.3 84

Power History - Data Set Sample of Power Consumed 85

Power Usage Statistics and History Web Enhancements as of
Oracle ILOM 3.0.4 86

Power Usage Statistics and Power History Web Enhancements as
of Oracle ILOM 3.0.14 87

CLI Power Consumption History Metrics 88

Power Consumption Threshold Notifications as of Oracle ILOM 3.0.4 89

Component Allocation Distribution as of Oracle ILOM 3.0.6 for Server SP
and CMM 90

Monitoring Server Power Allocated Components	90
Monitoring CMM Power Allocated Components	92
Component Power Allocation Special Considerations	94
Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.8 (Server SP)	95
Updated Server SP Power Allocation Web Procedure	96
Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.10 (CMM)	96
Revised CLI Power Allocation Properties as of Oracle ILOM 3.0.10	98
Power Budget as of Oracle ILOM 3.0.6 for Server SPs	99
Why Use a Power Budget?	100
Server Power Budget Properties as Oracle ILOM 3.0.6	101
Advanced Server Power Budget Features as of Oracle ILOM 3.0.6	101
Power Management --> Budget Tab Renamed to Limit Tab as of Oracle ILOM 3.0.8	103
Updated Power Limit Configuration Procedure	105
Power Supply Redundancy for CMM Systems as of Oracle ILOM 3.0.6	105
Platform-Specific CMM Power Metrics as of Oracle ILOM 3.0.6	106
Remote Host Management Operations	109
Remote Power Control	110
Host Control - Boot Device on x86 Systems	110
Oracle ILOM Operations for LDom Configurations on SPARC Servers	111
Remote Redirection Console Options	111
Oracle ILOM Host Maintenance and Diagnostics Options	113
Host Maintenance Operations	113
Host Diagnostic Options	114
Example Setup of Dynamic DNS	115

Dynamic DNS Overview 115

Example Dynamic DNS Configuration 117

Assumptions 117

▼ Configure and Start the DHCP and DNS Servers 117

References 119

Glossary 121

Index 139

Using This Documentation

This concepts guide describes the Oracle Integrated Lights Out Manager (ILOM) 3.0 daily management features that are common to Oracle's Sun rack-mounted servers, server modules, and CMMs supporting Oracle ILOM 3.0.

Use this guide in conjunction with other guides in the Oracle ILOM 3.0 Documentation Collection. This guide is written for technicians, system administrators, authorized service providers, and users who have experience managing system hardware.

This section includes the following topics:

- “Documentation and Feedback” on page ix
- “Product Downloads” on page x
- “Oracle ILOM 3.0 Firmware Version Numbering Scheme” on page xi
- “Documentation, Support, and Training” on page xii

Documentation and Feedback

You can download the Oracle ILOM 3.0 Documentation Collection at:
<http://www.oracle.com/pls/topic/lookup?ctx=E19860-01&id=homepage>

Application	Title	Format
Online Documentation Set	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 HTML Documentation Collection</i>	HTML
Quick Start	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Quick Start Guide</i>	PDF
Remote KVMs	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Remote Redirection Consoles — CLI and Web Guide</i>	PDF
Daily Management Features	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Daily Management — Concepts Guide</i>	PDF
Daily Management Web Procedures	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Daily Management — Web Procedures Guide</i>	PDF
Daily Management CLI Procedures	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Daily Management — CLI Procedures Guide</i>	PDF
Protocol Management	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Protocol Management — SNMP, IPMI, CIM, WS-MAN Guide</i>	PDF
CMM Administration	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CMM Administration Guide for Sun Blade 6000 and 6048 Modular Systems</i>	PDF
Maintenance and Diagnostics	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Maintenance and Diagnostics — CLI and Web Guide</i>	PDF
Late Breaking Information	<i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Feature Updates and Release Notes</i>	PDF

You can provide feedback on this documentation at:

<http://www.oracle.com/technetwork/enterprise/ilo30/feedback.html>

Product Downloads

Updates to the Oracle ILOM 3.0 firmware are available through standalone software updates that you can download from the My Oracle Support (MOS) web site for each Sun server or Sun blade chassis system. To download these software updates from the MOS web site, see the instructions that follow.

▼ Download Product Software and Firmware

1. Go to <http://support.oracle.com>.
2. Sign in to My Oracle Support.
3. At the top of the page, click the Patches and Updates tab.
4. In the Patches Search box, select Product or Family (Advanced Search).
5. In the Product? Is field, type a full or partial product name, for example Sun Fire X4470, until a list of matches appears, then select the product of interest.
6. In the Release? Is pull down list, click the Down arrow.
7. In the window that appears, click the triangle (>) by the product folder icon to display the choices, then select the product of interest.
8. In the Patches Search box, click Search.
A list of product downloads (listed as patches) appears.
9. Select the patch name of interest, for example Patch 10266805 for the ILOM and BIOS portion of the Sun Fire X4470 SW 1.1 release.
10. In the right-side pane that appears, click Download.

Oracle ILOM 3.0 Firmware Version Numbering Scheme

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

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

For example, Oracle ILOM 3.1.2.1.a would designate:

- Oracle ILOM 3 as the major version

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

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

Documentation, Support, and Training

These web sites provide additional resources:

- Documentation (<http://www.oracle.com/technetwork/indexes/documentation/index.html>)
- Support (<https://support.oracle.com>)
- Training (<https://education.oracle.com>)

Oracle ILOM Overview

Description	Links
Learn about Oracle ILOM features and functionality.	<ul style="list-style-type: none">• “What Is Oracle ILOM?” on page 2• “What Does Oracle ILOM Do?” on page 2• “Oracle ILOM Features and Functionality” on page 4• “New Features in Oracle ILOM 3.0” on page 5
Get started with using Oracle ILOM 3.0 user accounts.	<ul style="list-style-type: none">• “User Accounts – Backward Compatibly” on page 6• “Preconfigured User Accounts” on page 7
Identify Oracle ILOM 3.0 user interfaces, device management options, and ways you can publish system messages to Oracle ILOM users.	<ul style="list-style-type: none">• “Oracle ILOM Supported Interfaces” on page 9• “Oracle ILOM on the Server SP and CMM” on page 10• “System Banner Messages” on page 10

Related Information

- [Oracle ILOM 3.0 Daily Management CLI Procedures](#), overview CLI
- [Oracle ILOM 3.0 Daily Management Web Procedures](#), overview web interface
- [Oracle ILOM 3.0 Protocol Management](#), management using SNMP
- [Oracle ILOM 3.0 Protocol Management](#), management using IPMI
- [Oracle ILOM 3.0 Protocol Management](#), CIM and WS-MAN
- [Oracle ILOM 3.0 Remote Redirection Consoles](#), remote redirection consoles
- [Oracle ILOM 3.0 Maintenance and Diagnostics](#), host maintenance operations, host diagnostics

What Is Oracle ILOM?

Oracle's Integrated Lights Out Manager (ILOM) provides advanced service processor hardware and software that you can use to manage and monitor your Oracle Sun servers. Oracle ILOM's dedicated hardware and software is preinstalled on a variety of Oracle Sun server platforms, including x86-based Sun Fire servers, Sun Blade modular chassis systems, Sun Blade server modules, as well as on SPARC-based servers. Oracle ILOM is a vital management tool in the data center and can be used to integrate with other data center management tools already installed on your systems.

Oracle ILOM is supported on many Oracle systems enabling users to experience a single, consistent, and standards-based service processor (SP) across all Oracle Sun server product lines. This means you will have:

- Single, consistent system management interfaces for operators
- Rich protocol and standards support
- Broadening third-party management support
- System management functions integrated into Oracle's Sun servers at no extra cost

What Does Oracle ILOM Do?

Oracle ILOM enables you to actively manage and monitor the server independently of the operating system state, providing you with a reliable lights out management (LOM) system. With Oracle ILOM, you can proactively:

- Learn about hardware errors and faults as they occur
- Remotely control the power state of your server
- View the graphical and non-graphical consoles for the host
- View the current status of sensors and indicators on the system
- Determine the hardware configuration of your system
- Receive generated alerts about system events in advance through IPMI PEs, SNMP traps, or email alerts.

The Oracle ILOM service processor (SP) runs its own embedded operating system and has a dedicated Ethernet port, which together provide out-of-band management capability. In addition, you can access Oracle ILOM from the server's host operating

system (Solaris, Linux, and Windows). Using Oracle ILOM, you can remotely manage your server as if you were using a locally attached keyboard, monitor, and mouse.

Oracle ILOM automatically initializes as soon as power is applied to your server. It provides a full-featured, browser-based web interface and has an equivalent command-line interface (CLI). There is also an industry-standard SNMP interface and IPMI interface.

You can easily integrate these management interfaces with other management tools and processes that you might have working already with your servers, such as Oracle Enterprise Ops Center. This easy-to-use system management platform for Solaris and Linux provides the tools that you need to efficiently manage systems on your network. Oracle Enterprise Ops Center can discover new and existing systems on your network, update firmware and BIOS configurations, provision the operating environment with off-the-shelf distributions or Solaris images, manage updates and configuration changes, and remotely control key aspects of the service processor such as boot control, power status, and indicator lights. For more information about Oracle Enterprise Ops Center, go to:

<http://www.oracle.com/technetwork/oem/enterprise-manager/documentation/index.html>

In addition, you can integrate Oracle ILOM with these third-party management tools:

- Oracle Hardware Management Connector 1.2 for Altiris Deployment Solution
- BMC PATROL 6.9
- CA Unicenter Network and Systems Management (NSM)
- HP OpenView Operations for UNIX
- HP OpenView Operations for Windows
- HP Systems Insight Manager
- IBM Director
- IBM Tivoli Enterprise Console
- IBM Tivoli Monitoring (ITM)
- IBM Tivoli Netcool/OMNIBus
- IPMItool 1.8.10.3 for Microsoft Windows 2003
- Microsoft Operations Manager 2005
- Microsoft System Management
- Microsoft Systems Center Operations Manager 2007
- Sun Deployment Pack 1.0 for Microsoft System Center Configuration Manager 2007
- Sun Update Catalog for Microsoft System Center Configuration Manager 2007
- Sun IPMI System Management Driver for Server 2003 prior to R2

■ Sun ILOM Common SNMP MIBs

A description of these third-party system management tools and their support for Oracle's Sun systems is available at:

<http://www.oracle.com/technetwork/server-storage/servermgmt/downloads/index.html>

Oracle ILOM Features and Functionality

Oracle ILOM offers a full set of features, functions, and protocols that will help you monitor and manage your server systems.

TABLE: Oracle ILOM Features and Functionality

Oracle ILOM Feature	What You Can Do
Dedicated service processor and resources	<ul style="list-style-type: none">• Manage the server without consuming system resources.• Continue to manage the server using standby power even when the server is powered off.
Simple Oracle ILOM initial configuration	<ul style="list-style-type: none">• ILOM automatically learns the network address of the server SP or CMM using IPv4 and IPv6 default settings.
Downloadable firmware updates	<ul style="list-style-type: none">• Download firmware updates using the browser-based web interface.
Remote hardware monitoring	<ul style="list-style-type: none">• Monitor system status and event logs.• Monitor customer-replaceable units (CRUs) and field-replaceable units (FRUs), including power supplies, fans, host bus adapters (HBAs), disks, CPUs, memory, and motherboard.• Monitor environmentals (component temperatures).• Monitor sensors, including voltage and power.• Monitor indicators (LEDs).
Hardware and FRU inventory and presence	<ul style="list-style-type: none">• Identify installed CRUs and FRUs and their status.• Identify part numbers, versions, and product serial numbers.• Identify NIC card MAC addresses.
Remote KVMs	<ul style="list-style-type: none">• Redirect the system serial console via serial port and LAN.• Access keyboard, video, and mouse (KVM) on remote x86 systems and on some SPARC systems.• Redirect the OS graphical console to a remote client browser.• Connect a remote CD/DVD/floppy to the system for remote storage.

TABLE: Oracle ILOM Features and Functionality (*Continued*)

Oracle ILOM Feature	What You Can Do
System power control and monitoring	<ul style="list-style-type: none">• Power the system on or off, either locally or remotely.• Force power-off for emergency shutdown or perform a graceful shutdown to shut down the host operating system before power off.
Configuration and management of user accounts	<ul style="list-style-type: none">• Configure local user accounts.• Authenticate user accounts using LDAP, LDAP/SSL, RADIUS, and Active Directory.
Error and fault management	<ul style="list-style-type: none">• Monitor system BIOS, POST, and sensor messages.• Log events in a consistent method for all “service” data.• Monitor hardware and system-related errors, as well as ECC memory errors, reported into SP logs, syslog, and remote log-host.
System alerts, including SNMP traps, IPMI PEs, remote syslog, and email alerts	<ul style="list-style-type: none">• Monitor components using industry-standard SNMP commands and the IPMItool utility.

New Features in Oracle ILOM 3.0

Oracle ILOM 3.0 is enhanced with many new features and functions that were not available in Oracle ILOM 2.x, including improved security, improved usability, and easier integration into your data center environment. The following table identifies some of the new features provided in Oracle ILOM 3.0.

TABLE: Oracle ILOM 3.0 New Features

Category	Feature
General Functionality	
	DNS support
	Timezone support
	Configuration backup and restore
	Restore to factory defaults
	Enhanced LDAP and LDAP/SSL support
	Java-based remote storage CLI
	Power management capabilities

TABLE: Oracle ILOM 3.0 New Features (*Continued*)

Category	Feature
	Ability to generate new SSH keys
Scalability and Usability	
	User-configurable filtering of hardware monitoring information in CLI and web interface
	Use host name to access other services by name, such as LDAP, Active Directory, LDAP/SSL
Security	
	More granular user roles
	Predefined <code>root</code> and <code>default</code> accounts
	User SSH key authentication
	Ability to disable the network management port when you are using only the serial port
	Ability to disable individual services, such as IPMI, SSH, and KVMS, so that the port is closed
Serviceability	
	Data collection utility to diagnose system problems

For more information about new point release features implemented after Oracle ILOM 3.0, see the *Oracle ILOM 3.0 Feature Updates and Release Notes*.

User Accounts – Backward Compatibly

For Oracle ILOM 3.0, user roles are implemented to control user privileges. However, for backward compatibility, Oracle ILOM 2.x style user accounts (which have either Administrator or Operator privileges) are still supported.

For more information about Oracle ILOM 3.0 user roles, see [“Oracle ILOM 3.0 User Account Roles” on page 32](#).

Preconfigured User Accounts

Oracle ILOM 3.0 provides the following two preconfigured accounts:

- “root User Account” on page 7
- “default User Account” on page 8

root User Account

The `root` user account is persistent and is available on all interfaces (web interface, CLI, SSH, serial console, and IPMI) unless you choose to delete the `root` account. The `root` account provides built-in administrative privileges (read and write) for all Oracle ILOM features, functions, and commands.

To log in to Oracle ILOM, use the following `root` account user name and password:

User name: **root**

Password: **changeme**

To prevent unauthorized access to your system, you should change the `root` password (`changeme`) on each service processor (SP) or chassis monitoring module (CMM) installed in your system. Alternatively, you can delete the `root` account to secure access to your system. However, before you delete the `root` account, you must set up a new user account or configure a directory service so that you will be able to log in to Oracle ILOM.

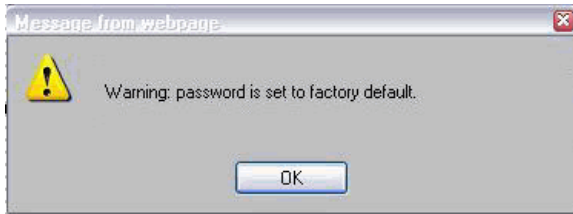
root Factory Default Password Warning Message

As of Oracle ILOM 3.0.6, when the `root` password in Oracle ILOM is set to the factory default, a warning appears on the Oracle ILOM CLI and web interface.

For example:

- In the Oracle ILOM web interface, a warning link appears in the page header. Placing your pointer over the link displays the warning message or clicking the warning link displays the warning message in a dialog box.





- In the Oracle ILOM CLI, the following factory default warning message appears after logging in to Oracle ILOM.

```
Password:
Waiting for daemons to initialize...
Daemons ready
Oracle (TM) Integrated Lights Out Manager

Version 3.0.0.0 r46636
Copyright 2009 Sun Microsystems, Inc. All Rights reserved.
Use is subject to license terms.
```

default User Account

The default user account is used for password recovery. The default user account is available through the serial console only and you must prove physical presence at the server to use the default user account. The default user account cannot be changed or deleted.

If you delete the `root` account before you have configured another user account to log in to Oracle ILOM, you can use the default account as an alternative way to log in and re-create the `root` account. To re-create the `root` user account, use the normal Oracle ILOM user commands to create a new account. For information about how to create a user account, see the section about Add User Account in the *Oracle ILOM 3.0 Quick Start Guide*.

For password recovery, use the following user name and password to log in using the default account:

User name: **default**

Password: **defaultpassword**

Oracle ILOM Supported Interfaces

To access all of Oracle ILOM's features and functions, you can choose to use a browser-based web interface, a command-line interface, or industry-standard protocols.

- **Web interface** – The web interface enables you to access the Oracle ILOM SP or CMM through a web browser. From the Oracle ILOM's web interface, you can perform daily system management operations remotely. Additionally, from the web interface, you can launch tools to redirect KVMS, or to perform maintenance and diagnostic operations.
- **Command-line interface (CLI)** – Using an SSH client, you can access the Oracle ILOM CLI on the server SP or CMM. This command-line interface enables you to perform server management operations remotely using industry-standard DMTF-style keyboard commands and scripting protocols.
- **Intelligent Platform Management Interface (IPMI)** – IPMI is an open, industry-standard interface that was designed for the management of server systems over a number of different types of networks. IPMI functionality includes field-replaceable unit (FRU) inventory reporting, system monitoring, logging of system events, system recovery (including system resets and power-on and power-off capabilities), and alerting.

For more information about using IPMI to monitor or manage your Oracle Sun server, see the *Oracle ILOM 3.0 Protocol Management Reference Guide*.

- **WS-Management/CIM** – As of version 3.0.8, Oracle ILOM supports the use of the Distributed Management Task Force (DMTF) Web Services for Management (WS-Management) protocol and Common Information Model (CIM). The support for these DMTF standards in Oracle ILOM enables developers to build and deploy network management applications to monitor and manage information about Oracle's Sun system hardware.

For more information about WS-Management/CIM, refer to the *Oracle ILOM 3.0 Protocol Management Reference Guide*.

- **Simple Network Management Protocol (SNMP) interface** – Oracle ILOM also provides an SNMP v3.0 interface for third-party applications such as HP OpenView and IBM Tivoli. Some of the MIBs supported by Oracle ILOM 3.0 include:
 - SUN-PLATFORM-MIB
 - SUN-ILOM-CONTROL-MIB
 - SUN-HW-TRAP-MIB
 - SUN-ILOM-PET-MIB
 - SNMP-FRAMEWORK-MIB (9RFC2271.txt)

- SNMP-MPD-MIB (RFC2572)
- System and SNMP groups from SNMPv2-MIB (RFC1907)
- entPhysicalTable from ENTITY-MIB (RFC2737)

For a complete list of SNMP MIBs supported and used by Oracle ILOM, refer to the *Oracle ILOM 3.0 Protocol Management Reference Guide*.

For more information about Oracle ILOM interfaces, refer to the Overview sections in the *Oracle ILOM 3.0 CLI Procedures Guide* and *Oracle ILOM 3.0 Web Procedures Guide*.

Oracle ILOM on the Server SP and CMM

Oracle ILOM supports the following two ways of managing a system:

- Using the service processor (SP) directly – Communicating directly with the rackmounted server SP or server module SP enables you to manage and monitor an individual server.
- Using the chassis monitoring module – Communicating directly with the CMM enables you to manage individual chassis components and an aggregate of components at the chassis level.

For more information about managing ILOM on the server SP and CMM using Oracle ILOM interfaces, refer to:

- *Oracle ILOM 3.0 CLI Procedures Guide*, CLI Overview
- *Oracle ILOM 3.0 Web Procedures Guide*, Web Interface Overview

System Banner Messages

As of Oracle ILOM 3.0.8, system administrators can create banner messages and display them on the Login page.

Creating and displaying banner messages in Oracle ILOM is optional. However, system administrators can use this capability whenever there is a need to share information about system updates, system policies, or other important announcements. Examples of where (Login page or after login) the banner message appear in Oracle ILOM after they have been created are shown in [FIGURE: Login Page – Connect Banner Example – Web Interface on page 11](#), [FIGURE: After Logging In - Banner Message Example - Web Interface on page 12](#), and [FIGURE: Banner Message Example - CLI on page 12](#).

For instructions about how to create the banner messages in Oracle ILOM, refer to the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

FIGURE: Login Page – Connect Banner Example – Web Interface

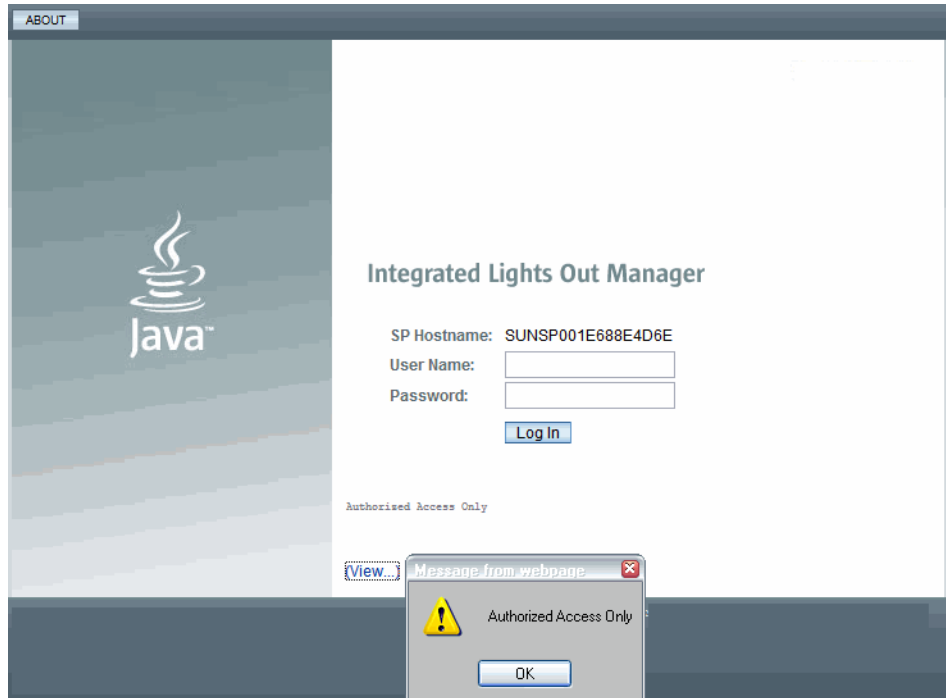


FIGURE: After Logging In - Banner Message Example - Web Interface

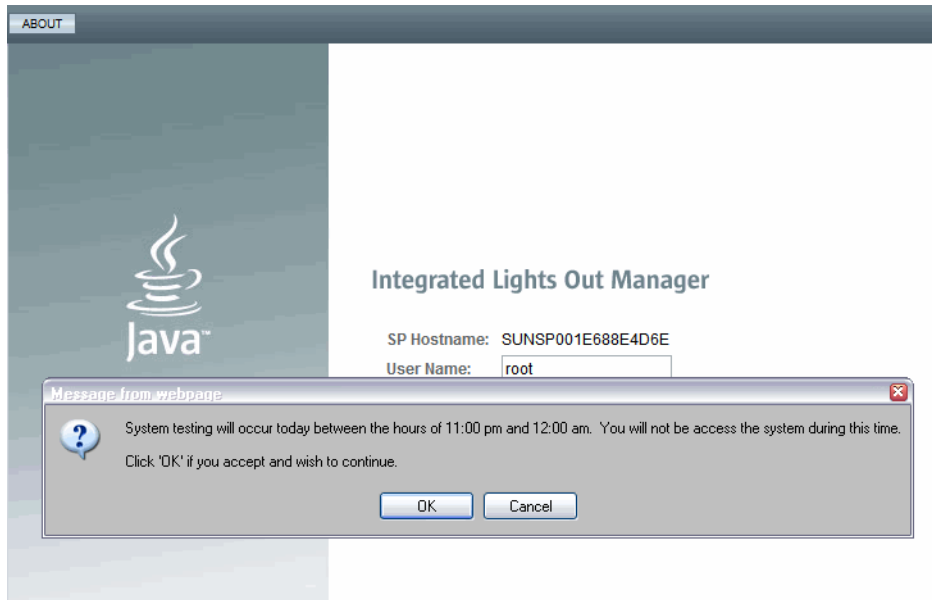


FIGURE: Banner Message Example - CLI

```
login as: root
Using keyboard-interactive authentication.
Password:

Integrated Lights Out Manager

Version 3.0.0.0 r55502

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

System testing will occur today between the hours of 11:00 pm and 12:00 am. You
will not be access the system during this time.

Do you agree to the above terms and wish to continue? (y/n) █
```


Network Configurations

Description	Links
Learn about Oracle ILOM network management and connection methods.	<ul style="list-style-type: none">• “Oracle ILOM Network Management” on page 14
Learn about Oracle ILOM network communication settings and network port assignments.	<ul style="list-style-type: none">• “Oracle ILOM Communication Settings” on page 18• “Default Network Port Used By Oracle ILOM” on page 16• “Switch Serial Port Console Output (Serial Port Owner)” on page 18• “SP Management Port – Recommended Practice for Spanning Tree Parameters” on page 19
Learn about configuring Oracle ILOM in an IPv4 network environment.	<ul style="list-style-type: none">• “Network Configurations for IPv4” on page 19
Learn about configuring Oracle ILOM in a dual-stack IPv4/IPv6 network environment.	<ul style="list-style-type: none">• “Dual-Stack Network Configurations for IPv4 and IPv6 (ILOM 3.0.12)” on page 20
Learn about configuring the Local Interconnect Interface.	<ul style="list-style-type: none">• “Local Interconnect Interface: Local Connection to ILOM From Host OS” on page 24

Related Information

- *Oracle ILOM 3.0 Daily Management CLI Procedures*, configuring communication settings
- *Oracle ILOM 3.0 Daily Management Web Procedures*, configuring communication settings
- *Oracle ILOM 3.0 Protocol Management Reference*, configuring communication settings

Oracle ILOM Network Management

You can establish communication with Oracle ILOM through a console connection to the serial management port on the server or chassis monitoring module (CMM), or through an Ethernet connection to the network management port on the server or CMM.

A dedicated network management port will help you manage your server platform optimally with Oracle ILOM. Using the network management port, traffic destined for Oracle ILOM is kept separate from any data transfers made by the host operating system.

Refer to your platform documentation to determine how to connect to your network management port.

You can use Dynamic DNS to automatically assign a host name and IP address on new Oracle ILOM installations based on the system's serial number. See ["Example Setup of Dynamic DNS" on page 115](#) for an overview of Dynamic DNS and configuration instructions.

This topic contains the following information:

- ["Oracle ILOM Connection Methods" on page 14](#)
- ["Initial Setup Worksheet" on page 15](#)
- ["Default Network Port Used By Oracle ILOM" on page 16](#)
- ["Switch Serial Port Console Output \(Serial Port Owner\)" on page 18](#)

Oracle ILOM Connection Methods

The way in which you connect to Oracle ILOM depends on your server platform. Refer to your platform documentation for details.

The following table lists the different methods you can use to connect to Oracle ILOM.

TABLE: Oracle ILOM Connection Methods

Connection Method	Rack-Mounted	Blade	Supported Interface	Description
Ethernet network management connection	Yes	Yes	CLI and web interface	Connect to the Ethernet network management port. You must know Oracle ILOM's host name or IP address.
Serial connection	Yes	Yes	CLI only	Connect directly to the serial management port.
Local Interconnect Interface (as of Oracle ILOM 3.0.12)	Verify support for this feature in your platform Oracle ILOM Supplement Guide or Administration Guide.			Enables you to connect to Oracle ILOM directly from the host operating system without the need of a physical network connection to the server SP. This feature is not supported on all Sun servers. For more information, see "Local Interconnect Interface: Local Connection to ILOM From Host OS" on page 24.

Note – Oracle ILOM supports a maximum of 10 active user sessions, including serial, Secure Shell (SSH), and web interface sessions per service processor (SP). Some SPARC systems support a maximum of only 5 active user sessions per SP.

Initial Setup Worksheet

The following table describes the information that you need to establish initial communication with Oracle ILOM

TABLE: Initial Setup Worksheet to Establish Communication With Oracle ILOM

Information for Setup	Requirement	Description
Management Connection–Serial	Mandatory - <i>if network environment does not support IPv4 DHCP or IPv6 stateless</i>	Oracle ILOM, by default, learns the IPv4 network address using DHCP and the IPv6 network address using IPv6 stateless. If your network environment does not support IPv4 DHCP or IPv6 stateless, you must establish a local serial console connection to Oracle ILOM via the serial management port on the server or Chassis Monitoring Module (CMM). If your network environment supports IPv4 DHCP or IPv6 stateless, see the setup information for Management Connection - Ethernet (below). For more information about how to attach a serial console to a server or CMM, refer to your platform documentation.
Management Connection–Ethernet	Optional	You can access Oracle ILOM remotely when using the IP address, host name, or local link address assigned to the server SP. This method requires a connection from your local area network to the Ethernet network management port (NET MGT) on the server or CMM. To establish a physical network connection to your server, refer to the installation documentation provided for your server or CMM.
SP Host Name Assignment	Optional	You can assign a meaningful host name to a server SP. For more information, see the <i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide</i> or the <i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide</i> .
System Identifier Assignment	Optional	You can assign a system identifier (meaningful name) to a Sun server. For more information, see the <i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide</i> or the <i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide</i> .
Dynamic DNS Configuration	Optional	You can configure Dynamic DNS to support the use of host names to access server SPs. For example information about setting up Dynamic DNS, see “Example Setup of Dynamic DNS” on page 115 . For Dynamic DNS configuration procedures, see <i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide</i> .

Default Network Port Used By Oracle ILOM

The following table identifies the default network ports used by Oracle ILOM. Most of these network ports are configurable.

Note – [TABLE: Oracle ILOM Network Ports on page 17](#) identifies default network ports as of Oracle ILOM 3.0.6. Some network ports might not be available if you are not using Oracle ILOM 3.0.6 or a later version of Oracle ILOM.

TABLE: Oracle ILOM Network Ports

Port	Protocol	Application
Common Network Ports		
22	SSH over TCP	SSH - Secure Shell
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol (outgoing)
80	HTTP over TCP	Web (user-configurable)
123	NTP over UDP	NTP - Network Time Protocol (outgoing)
161	SNMP over UDP	SNMP - Simple Network Management Protocol (user-configurable)
162	IPMI over UDP	IPMI - Platform Event Trap (PET) (outgoing)
389	LDAP over UDP/TCP	LDAP - Lightweight Directory Access Protocol (outgoing; user-configurable)
443	HTTPS over TCP	Web (user-configurable)
514	Syslog over UDP	Syslog - (outgoing)
623	IPMI over UDP	IPMI - Intelligent Platform Management Interface
546	DHCP over UDP	DHCP - Dynamic Host Configuration Protocol (client)
1812	RADIUS over UDP	RADIUS - Remote Authentication Dial In User Service (outgoing; user-configurable)
SP Network Ports		
5120	TCP	Oracle ILOM Remote Console: CD
5121	TCP	Oracle ILOM Remote Console: Keyboard and Mouse
5123	TCP	Oracle ILOM Remote Console: Diskette
5555	TCP	Oracle ILOM Remote Console: Encryption
5556	TCP	Oracle ILOM Remote Console: Authentication
6481	TCP	Oracle ILOM Remote Console: Servicetag Daemon
7578	TCP	Oracle ILOM Remote Console: Video
7579	TCP	Oracle ILOM Remote Console: Serial
CMM Network Ports		

TABLE: Oracle ILOM Network Ports (Continued)

Port	Protocol	Application
8000 - 8023	HTTP over TCP	Oracle ILOM drill-down to server modules (blades)
8400 - 8423	HTTPS over TCP	Oracle ILOM drill-down to server modules (blades)
8200 - 8219	HTTP over TCP	Oracle ILOM drill-down to NEMs
8600 - 8619	HTTPS over TCP	Oracle ILOM drill-down to NEMs

Switch Serial Port Console Output (Serial Port Owner)

Oracle ILOM, by default, displays the serial port output from the server to the server SP console (SER MGT port). On some Sun servers, however, you can choose to switch the owner of the serial port output between the server SP and the Host console (COMM1 port).

Note – Switching the serial port output owner to the Host console is helpful during windows debugging situations, as this output configuration enables you to view non-ASCII character traffic from the Host console.

For more information and procedures for switching the serial port output, see the *Oracle ILOM 3.0 CLI Procedures, Switch Serial Port Output*.

Oracle ILOM Communication Settings

You can use the Oracle ILOM CLI interface, web interface, or SNMP to manage Oracle ILOM's communication settings, including network, serial port, web, and Secure Shell (SSH) configurations. Oracle ILOM lets you view and configure system host names, IP addresses, DNS settings, and serial port settings. You also can enable or disable HTTP or HTTPS web access, and enable or disable SSH.

For more information and procedures for managing Oracle ILOM communication settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

SP Management Port – Recommended Practice for Spanning Tree Parameters

Since the SP network management port is not designed to behave like a switch port, the SP network management port does not support switch port features like spanning-tree portfast.

When configuring spanning tree parameters, consider these recommendations:

- The port used to connect the SP network management port to the adjacent network switch should always treat the SP network management port as a host port.
- The spanning tree option on the port connecting to the adjacent network switch should either be disabled entirely or at a minimum configured with the following parameters:

Spanning Tree Parameter	Recommended Setting
portfast	Enable this interface to immediately move to a forwarding state.
bpdufilter	Do not send or receive BPDUs on this interface.
bpduguard	Do not accept BPDUs on this interface.
cdp	Do not enable the discovery protocol on this interface.

Network Configurations for IPv4

Oracle ILOM, by default, uses IPv4 DHCP to learn the IPv4 address for the server SP. If DHCP is not supported in your network environment or if you prefer to set up a static IPv4 address, you can configure the IPv4 network settings in Oracle ILOM from the CLI or web interface.

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

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, and Gateway.

State: Enabled

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

IP Discovery Mode: DHCP Static

IP Address:

Netmask:

Gateway:

For instructions on how to configure the network settings in Oracle ILOM for IPv4, refer to one of the following Oracle ILOM procedure guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide (820-6411), Chapter 4.*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide (820-6412), Chapter 4.*

Dual-Stack Network Configurations for IPv4 and IPv6 (ILOM 3.0.12)

Oracle ILOM, by default, uses IPv6 stateless to learn the IPv6 address for the server SP. If IPv6 stateless is not supported in your network environment or if you prefer to use another IPv6 network setting to communicate with Oracle ILOM, you can modify the IPv6 network settings using the Oracle ILOM CLI or web interface.

Note – As of Oracle ILOM 3.0.12, dual-stack IPv4 and IPv6 network settings are supported on some servers. Verify support of the IPv6 settings in your platform Oracle ILOM Supplement Guide or Administration Guide.

This topic includes the following information:

- [“Oracle ILOM IPv6 Enhancements” on page 21](#)
- [“Legacy Sun Server Platforms Not Supporting IPv6” on page 24](#)

Oracle ILOM IPv6 Enhancements

Oracle ILOM enhancements for IPv6 include:

- Support for a larger 128-bit IPv6 addressing space.
- Acceptance of IPv6 addresses in designated text entry fields and URLs throughout Oracle ILOM.

Note – IPv6 addresses are written with hexadecimal digits and colon separators like 2001:0db0:000:82a1:0000:0000:1234:abcd, as opposed to the dot-decimal notation of the 32-bit IPv4 addresses. IPv6 addresses are composed of two parts: a 64-bit subnet prefix, and a 64-bit host interface ID. To shorten the IPv6 address, you can: (1) omit all leading zeros and (2) replace one consecutive group of zeros with a double colon (::). For example: 2001:db0:0:82a1::1234:abcd

- Ability for Oracle ILOM to operate fully in a dual-stack IPv4 and IPv6 environment. Within a dual-stack network environment, Oracle ILOM is capable of responding to both IPv4 and IPv6 addresses that are concurrently configured for a device (server SP or CMM).
- Support for IPv6 protocols. As of Oracle ILOM 3.0.12, IPv6 protocol support includes: SSH, HTTP, HTTPS, Ping6, SNMP, JRC, NTP, KVMS, and all file transfer protocols (tftp, scp, ftp, and so on). Full support for all remaining IPv6 protocols is available as of Oracle ILOM 3.0.14.
- Support for the following IPv6 auto-configuration options are available for a device (server SP or CMM):

TABLE: IPv6 Address Auto-Configuration Options in Oracle ILOM

IPv6 Address Auto-Configurations	Description	Supported in Oracle ILOM Release:
Stateless (enabled by default)	When enabled, the IPv6 <code>Stateless</code> auto-configuration is run to learn the IPv6 address(es) for the device. Note - If you are running Oracle ILOM 3.0.12, this option appears as <code>stateless_only</code> in the CLI. If you are running Oracle ILOM 3.0.14 or later, this option appears as <code>stateless</code> in the CLI.	3.0.12

TABLE: IPv6 Address Auto-Configuration Options in Oracle ILOM

IPv6 Address Auto-Configurations	Description	Supported in Oracle ILOM Release:
DHCPv6 Stateless	When enabled, the DHCPv6 Stateless auto-configuration is run to learn the DNS and domain information for the device.	3.0.14
DHCPv6 Stateful	When enabled, the DHCPv6 Stateful auto-configuration is run to learn the IPv6 address(es) and DNS information for the device.	3.0.14
Disabled	When enabled, the Disabled state will only set the Link Local address in Oracle ILOM. Oracle ILOM will not run any of the IPv6 auto-configuration options to configure an IPv6 address.	3.0.12

Note – As of Oracle ILOM 3.0.14, you can enable more than one IPv6 auto-configuration option to run at the same time with the exception of enabling these two auto-configuration options: to run at the same time: DHCPv6 Stateless and DHCPv6 Stateful.

- Ability to obtain routable IPv6 addresses from any of the following IPv6 network configurations:
 - Stateless auto-configuration (requires a network router configured for IPv6)
 - DHCPv6 Stateful auto-configuration
 - Manual configuration of single static IPv6 address.
- Support for reporting a Link-Local IPv6 address and up to 10 auto-configured IPv6 addresses per device.

Note – The Link-Local IPv6 address is always shown in Oracle ILOM under the /network/IPv6 target or on the Network Settings page. This address is a non-routable address that you can use to connect to the Oracle ILOM SP (or the CMM) from another IPv6 enabled node on the same network.

- Availability of a network configuration testing tool for IPv6 (Ping6).

Dual-Stack Network Options in Oracle ILOM CLI and Web Interface

The settings for configuring Oracle ILOM in a dual-stack IPv4 and IPv6 network environment are accessible for the server SP (web and CLI) or CMM (CLI only). See the following figure for an example of the dual-stack IPv4 and IPv6 web interface properties available for a server SP.

The screenshot shows the Oracle ILOM web interface with the following configuration details:

- System Information** | **System Monitoring** | **Power Management** | **Storage** | **Configuration** | **User Management** | **Remote Control** | **Maintenance**
- System Management Access | Alert Management | **Network** | DNS | Serial Port | Clock | Timezone | Syslog | SMTP Client | Policy
- 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, and Gateway. You can also configure 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:
- IPv4**
- IP Discovery Mode: DHCP Static
- IP Address:
- Netmask:
- Gateway:
- IPv6**
- IPv6 State: Enabled
- Autoconfig: Stateless DHCPv6 stateless DHCPv6 stateful
- Link-Local IP Address: fe80::214:4fff:feca:5f7e/64
- Static IP Address:
- Gateway: fe80::211:5dff:febe:5000/128
- Dynamic Addresses**

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

-

Note – The dual-stack IPv4 and IPv6 properties for the CMM are only accessible from the CLI. However, you can access the dual-stack IPv4 and IPv6 properties from the CMM web interface for the individual server SPs.

For a brief description of the IPv6 configuration options, see [TABLE: IPv6 Address Auto-Configuration Options in Oracle ILOM on page 21](#).

For instructions on how to configure the dual-stack network settings in Oracle ILOM for IPv4 and IPv6, refer to one of the following Oracle ILOM procedure guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411), Chapter 4.
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412), Chapter 4.

Legacy Sun Server Platforms Not Supporting IPv6

The following table identifies the legacy Sun server platforms that will not support IPv6 network configurations in Oracle ILOM.

Sun Platform	Server Model
SPARC Enterprise	<ul style="list-style-type: none">• T5440• T5220• T5120• T5140• T5240• T6340
x86 Sun Fire	<ul style="list-style-type: none">• X4140• X4150• X4240• X4440• X4450• X4600• X4600 M2• X4640

Local Interconnect Interface: Local Connection to ILOM From Host OS

As of Oracle ILOM 3.0.12, a communication channel known as the Local Interconnect Interface was added to Oracle ILOM to enable you to locally communicate with Oracle ILOM from the host operating system (OS) without the use of a network

management (NET MGT) connection to the server. The local interconnect feature to Oracle ILOM is particularly useful when you want to locally perform these Oracle ILOM tasks from the host operating system:

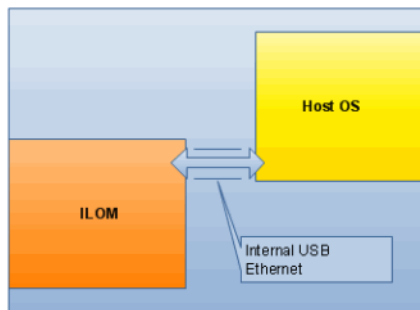
- Server management functions in Oracle ILOM that you would have typically performed from the Oracle ILOM CLI, web interface, or IPMI interface through the network management (NET MGT) connection on the server.
- Data transfers, such as firmware upgrades, to Oracle ILOM that you would have typically performed from the host over a Keyboard Controller Style (KCS) interface using IPMI flash tools. In particular, the Local Interconnect Interface to Oracle ILOM can provide a more reliable and faster data transfer rate than traditional KCS interfaces.
- To enable future server monitoring and fault detection tools from Oracle.

This topic includes the following information:

- [“Platform Server Support and Oracle ILOM Access Through the Local Interconnect Interface”](#) on page 25
- [“Local Interconnect Interface Configuration Options”](#) on page 26
- [“Local Host Interconnect Configuration Settings in Oracle ILOM”](#) on page 27

Platform Server Support and Oracle ILOM Access Through the Local Interconnect Interface

Oracle servers supporting the Local Interconnect Interface between Oracle ILOM and the host operating system are shipped from the factory with an internal USB Ethernet device installed.



The internal USB Ethernet device provides two network connection points that are known as the Oracle ILOM SP connection point and the host OS connection point. In order to establish a local connection to Oracle ILOM from the host operating system, each connection point (ILOM SP and host OS) must be either automatically or manually assigned a unique non-routable IPv4 address on the same subnet.

Note – By default, Oracle provides non-routable IPv4 addresses for each connection point (ILOM SP and host OS). Oracle recommends not changing these addresses unless a conflict exists in your network environment with the provided non-routable IPv4 addresses.

Note – Non-routable IPv4 addresses are considered secured private addresses that prevent external Internet users from navigating to your system.

To verify whether your server supports the Local Interconnect Interface feature in Oracle ILOM, refer to the Oracle ILOM Supplement guide or Administration guide that is provided with your server.

Local Interconnect Interface Configuration Options

In Oracle ILOM you can choose to either have the Local Interconnect Interface automatically configured for you or manually configured. Details about both of these configuration options are provided below.

■ Automatic Configuration (Recommended)

Oracle automates the configuration of the Local Interconnect Interface feature when you install the Oracle Hardware Management Pack 2.1.0 or later software. No configuration is necessary from Oracle ILOM in this case.

For more details about using the Oracle Hardware Management Pack 2.1.0 software to auto-configure the Local Interconnect Interface between the Oracle ILOM SP and the local host OS, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609).

Note – If you choose to auto-configure the Local Interconnect Interface using the Oracle Hardware Management Pack software, you should accept the factory defaults provided in Oracle ILOM for Local Host Interconnect.

■ Manually Configured (Advanced Users Only)

If you are an advanced network administrator and prefer not to auto-configure the Local Interconnect Interface by installing the Oracle Hardware Management Pack 2.1.0 or later software, you can manually configure the connection points on the Oracle ILOM SP and host operating system.

In order to manually configure the Local Interconnect Interface connection points, you must:

1. On the host operating side, ensure that an Ethernet driver for your host OS was provided by the OS distribution and installed on the server. After you have confirmed that the appropriate Ethernet driver was installed on your server and your operating system recognizes the internal USB Ethernet device, you must manually configure an IPv4 address for the host OS connection point.

For more details, see the Manual Host Configuration Guidelines in the *Oracle ILOM 3.0 CLI* or *Web Procedure* guides.

2. On the Oracle ILOM SP side, you must manually configure the Local Host Interconnect settings in Oracle ILOM. For more details about these settings, see [“Local Host Interconnect Configuration Settings in Oracle ILOM” on page 27](#). For procedural information describing how to configure the Local Interconnect Interface, see Chapter 3 of the *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* or the *Integrated Lights Out Manager (ILOM) Web Interface Procedures Guide*.

Local Host Interconnect Configuration Settings in Oracle ILOM

The Local Host Interconnect configuration settings in the Oracle ILOM web interface (or CLI) enable users with admin (a) role privileges to control the Local Interconnect Interface between the host OS and the Oracle ILOM SP.

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

Local Host Interconnect

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

Status: Host-Managed; Disabled [\(Configure\)](#)

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

For a description of the Local Host Interconnect settings provided in Oracle ILOM, see the following table.

TABLE: Local Host Interconnect Configuration Settings

Settings	Description
-Host Managed	<p>The <code>-Host Managed</code> setting, by default, is set to <code>-True</code>.</p> <p>When the <code>-Host Managed</code> setting is set to <code>-True</code> (enabled), Oracle ILOM permits the Oracle Hardware Management Pack configuration utility (known as <code>ilomconfig</code>) to auto-configure the connection points for the Oracle ILOM SP and the host OS on the Local Interconnect Interface.</p> <p>To prevent the Oracle Hardware Management Pack software from auto-configuring the connection points on the Local Interconnect Interface, the setting for <code>Host Managed</code> must be set to <code>False</code> (disabled).</p>
-State	<p>The <code>State</code> setting, by default, is disabled.</p> <p>When the setting for <code>State</code> is disabled, the Local Interconnect Interface feature between the Oracle ILOM SP and the host OS is disabled.</p> <p>When the setting for <code>State</code> is enabled, the Local Interconnect Interface feature between the Oracle ILOM SP and host OS is enabled.</p>
-IP Address	<p>Oracle ILOM, by default, provides a static non-routable IPv4 address (169.254.182.76) for the Oracle ILOM SP connection point on the Local Interconnect Interface.</p> <p>The IP address property is, by default, a read-only setting when the <code>-Host Managed</code> setting is set to <code>-True</code>.</p> <p>When the <code>-Host Managed</code> setting is disabled (or property value is set to <code>-False</code>), Oracle ILOM will allow you to modify the property value for the IPv4 address.</p> <p>Note - The default non-routable IPv4 address (169.254.182.76) should not be changed unless a conflict exists in your network environment with the default IPv4 address. When this address is left unchanged, this is the IP address you would use to locally connect to Oracle ILOM from the host operating system.</p>
-Netmask	<p>Oracle ILOM, by default, provides a static <code>-Netmask</code> address (255.255.255.0) for the Oracle ILOM SP connection point on the Local Interconnect Interface.</p> <p>The <code>-Netmask</code> property is, by default, a read-only setting when the <code>-Host Managed</code> setting is set to <code>-True</code>.</p> <p>When the <code>-Host Managed</code> setting is disabled (or property value is set to <code>-False</code>), Oracle ILOM will allow you to modify the property value for the <code>-Netmask</code> address.</p> <p>The default <code>-Netmask</code> address (255.255.255.0) should not be changed unless a conflict exists in your network environment with the default <code>-Netmask</code> address.</p>

TABLE: Local Host Interconnect Configuration Settings (*Continued*)

Settings	Description
-Service Processor MAC Address	The -Service Processor MAC Address is a read-only setting. This setting displays the MAC address assigned to the Oracle ILOM SP.
Host MAC Address	<p>The Host MAC Address is a read-only setting. This setting displays the MAC address assigned to the server and it represents how the host server sees the internal USB Ethernet device.</p> <p>Note - The internal USB Ethernet device is presented in the system as a traditional “Ethernet” interface. If you decide to manually configure the Local Interconnect Interface between the Oracle ILOM SP and the host OS, it might be necessary to use the host MAC address to determine which interface you will need to configure from the host OS side (like Solaris). For additional information about manually configuring the Local Interconnect Interface on the host OS connection point, see the Manual Host OS Configuration Guidelines for Local Interconnect Interface in the <i>Oracle ILOM 3.0 CLI or Web Procedures</i> guide.</p>
-Connection Type	The -Connection Type is a read-only setting. This setting indicates a USB Ethernet connection.

User Account Management

Description	Links
Learn about managing user accounts and roles	<ul style="list-style-type: none">• “Guidelines for Managing User Accounts” on page 31• “User Account Roles and Privileges” on page 32
Learn about establishing user credentials with Single Sign On	<ul style="list-style-type: none">• “Single Sign On” on page 33
Learn about password automation using SSH authentication.	<ul style="list-style-type: none">• “SSH User Key-Based Authentication” on page 34
Learn about using Active Directory to authenticate user accounts	<ul style="list-style-type: none">• “Active Directory” on page 34
Learn about user authentication using LDAP.	<ul style="list-style-type: none">• “Lightweight Directory Access Protocol” on page 36• “LDAP/SSL” on page 36
Learn about remote user authentication using RADIUS.	<ul style="list-style-type: none">• “RADIUS” on page 37

Related Information

- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage user accounts
- *Oracle ILOM 3.0 Daily Management Web Procedures*, manage user accounts
- *Oracle ILOM 3.0 Protocol Management Reference*, manage user accounts using SNMP
- *Oracle ILOM 3.0 Protocol Management Reference*, SNMP commands

Guidelines for Managing User Accounts

Apply the following general guidelines when you manage user accounts:

- Oracle ILOM supports a maximum of 10 active user sessions per service processor (SP). Some SPARC systems support a maximum of only 5 active user sessions per SP.
- The user name of an account must be at least four characters and no more than 16 characters. User names are case sensitive and must start with an alphabetical character. You can use alphabetical characters, numerals, hyphens, and underscores. Do not include spaces in user names.
- Each user account is assigned one or more advanced roles, which determine the privileges of the user account. Depending on the roles assigned to your user account, you can use the Oracle ILOM web interface, command-line interface (CLI), or SNMP to view account information and perform various administrative functions.
- You can either configure local accounts or you can have Oracle ILOM authenticate accounts against a remote user database, such as Active Directory, LDAP, LDAP/SSL, or RADIUS. With remote authentication, you can use a centralized user database rather than configuring local accounts on each Oracle ILOM instance.

For more information and procedures for managing user accounts, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

User Account Roles and Privileges

For Oracle ILOM 3.0, user roles are implemented to control user privileges. However, for backward compatibility, Oracle ILOM 2.x style user accounts (which have either Administrator or Operator privileges) are still supported.

Oracle ILOM 3.0 User Account Roles

Oracle ILOM 3.0 user accounts have defined roles that determine Oracle ILOM user access and rights. You can manage user accounts using the Oracle ILOM web interface or the CLI. The roles assigned to Oracle ILOM accounts are listed in [TABLE: Oracle ILOM 3.0 User Account Roles](#) on page 33.

TABLE: Oracle ILOM 3.0 User Account Roles

Roles	Definition	Privileges
a	Admin	A user who is assigned the Admin (a) role is authorized to view and change the state of Oracle ILOM configuration variables. With the exception of tasks that require Admin users to have User Management, Reset and Host Control and Console roles enabled.
u	User Management	A user who is assigned the User Management (u) role is authorized to create and delete user accounts, change user passwords, change roles assigned to other users, and enable/disable the physical-access requirement for the <code>default</code> user account. This role also includes authorization to set up LDAP, LDAP/SSL, RADIUS, and Active Directory.
c	Console	A user who is assigned the Console (c) role is authorized to access the Oracle ILOM Remote Console and the SP console and to view and change the state of the Oracle ILOM console configuration variables.
r	Reset and Host Control	A user who is assigned the Reset and Host Control (r) role is authorized to operate the system, which includes power control, reset, hot-plug, enabling and disabling components, and fault management. This role maps very closely to the Oracle ILOM 2.0 user with Operator privileges.
o	Read Only	A user who is assigned the Read Only (o) role is authorized to view the state of the Oracle ILOM configuration variables but cannot make any changes. Users assigned this role can also change the password and the Session Time-Out setting for their own user account.
s	Service	A user who is assigned the Service (s) role can assist Sun service engineers in the event that on-site service is required.

Single Sign On

Single Sign On (SSO) is a convenient authentication service that enables you to log in to Oracle ILOM once to establish your credentials, thus reducing the number of times you need to enter your password to gain access to Oracle ILOM. Single Sign On is enabled by default. As with any authentication service, authentication credentials are passed over the network. If this is not desirable, consider disabling the SSO authentication service.

SSH User Key-Based Authentication

Traditionally, automation of password authentication is made possible by SSH key-based authentication. Prior to the implementation of the SSH key-based authentication feature, users who logged in to the Oracle ILOM SP using SSH were required to supply a password interactively. An automatic mechanism for password authentication is most beneficial when you have multiple systems that require a similar update.

The primary capabilities afforded by SSH key-based authentication are as follows:

- Users are able to write scripts that automatically copy log files off of a service processor (SP) for archival and analysis.
- Users are able to write scripts that automatically and/or regularly execute SP commands over a network-based SSH connection from a remote system.

Thus, SSH key-based authentication enables you to accomplish both of the above activities through the use of scripts that execute without manual intervention and that do not include embedded passwords.

Regarding the use and handling of SSH keys, Oracle ILOM enables users to add generated keys to individual user accounts on the SP.

For more information and procedures for adding and deleting SSH keys, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Active Directory

Oracle ILOM supports Active Directory, the distributed directory service included with Microsoft Windows Server operating systems. Like an LDAP directory service implementation, Active Directory is used to authenticate user credentials.

Note – The service processor (SP) expects to communicate with the Active Directory server using a secure channel. To ensure security, the Active Directory server should be loaded with a certificate that can be presented during the SP user authentication process so that protocol negotiations can allow a private channel to be set up.

User Authentication and Authorization

Active Directory provides both authentication of user credentials and authorization of user access levels to networked resources. Active Directory uses authentication to verify the identity of a user before that user can access system resources. Active Directory uses authorization to grant specific access privileges to a user in order to control a user's rights to access networked resources. User access levels are configured or learned from the server based on the user's group membership in a network domain, which is a group of hosts identified by a specific Internet name. A user can belong to more than one group. Active Directory authenticates users in the order in which the user's domains were configured.

User Authorization Levels

Once authenticated, the user's authorization level can be determined in the following ways:

- In the simplest case, the user authorization of either Operator, Administrator, or Advanced Roles (see [“User Account Roles and Privileges” on page 32](#)) is learned directly through the Active Directory's configuration of the SP. Access and authorization levels are dictated by the `defaultrole` property. Setting up users in the Active Directory database requires only a password with no regard to group membership. On the SP, the `defaultrole` will be set to either Administrator, Operator, or the Advanced Role settings `a/u/c/r/o/s`. All users authenticated through Active Directory are assigned the privileges associated with the Administrator, Operator, or Advanced Roles based solely on this configuration.
- A more integrated approach is also available by querying the server. For configuration, the SP Administrator Group Tables, Operator Group Tables, or Custom Group Tables must be configured with the corresponding group names from the Active Directory server that will be used to determine access levels. Up to five Active Directory groups can be entered to designate an Administrator; another five can be used to assign Operator privileges; and up to five groups can be assigned to Custom Groups, which contain Advanced Roles (see [“User Account Roles and Privileges” on page 32](#)). Group membership of the user is used to identify the proper access level of either Administrator, Operator, or Advanced Roles by looking up each group name in the configured Active Directory tables on the SP. If the user's group list is not in either of the defined SP user groups, then access is denied. A user assigned to more than one group will receive the sum of all privileges.

For more information and procedures for configuring Active Directory settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*
-

Lightweight Directory Access Protocol

Oracle ILOM supports Lightweight Directory Access Protocol (LDAP) authentication for users, based on the OpenLDAP software. LDAP is a general-purpose directory service. A directory service is a centralized database for distributed applications designed to manage the entries in a directory. Thus, multiple applications can share a single user database. For more detailed information about LDAP, go to:

<http://www.openldap.org/>

For more information and procedures for configuring LDAP settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
 - *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
 - *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*
-

LDAP/SSL

LDAP/SSL offers enhanced security to LDAP users by way of Secure Socket Layer (SSL) technology. To configure LDAP/SSL in a SP, you need to enter basic data—such as primary server, port number, and certificate mode—and optional data such as alternate server or event or severity levels. You can enter this data using the LDAP/SSL configuration page of the Oracle ILOM web interface, the CLI, or SNMP.

For more information and procedures for configuring LDAP/SSL settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

RADIUS

Oracle ILOM supports Remote Authentication Dial-In User Service (RADIUS) authentication. RADIUS is an authentication protocol that facilitates centralized user administration. RADIUS provides many servers shared access to user data in a central database, providing better security and easier administration. A RADIUS server can work in conjunction with multiple RADIUS servers and other types of authentication servers.

RADIUS is based on a client-server model. The RADIUS server provides the user authentication data and can grant or deny access, and the clients send user data to the server and receive an “accept” or “deny” response. In the RADIUS client-server model, the client sends an Access-Request query to the RADIUS server. When the server receives an Access-Request message from a client, it searches the database for that user's authentication information. If the user's information is not found, the server sends an Access-Reject message and the user is denied access to the requested service. If the user's information is found, the server responds with an Access-Accept message. The Access-Accept message confirms the user's authentication data and grants the user access to the requested service.

All transactions between the RADIUS client and server are authenticated by the use of a specific text string password known as a shared secret. The client and server must each know the shared secret because it is never passed over the network. You must know the shared secret to configure RADIUS authentication for Oracle ILOM.

In order to use RADIUS authentication with Oracle ILOM, you must configure Oracle ILOM as a RADIUS client.

For more information and procedures for configuring RADIUS settings, see one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*

System Monitoring and Alert Management

Description	Links
Learn about system monitoring and management features in Oracle ILOM.	<ul style="list-style-type: none">• “System Monitoring” on page 40• “Sensor Readings” on page 41• “System Indicators” on page 41• “Component Management” on page 42• “Fault Management” on page 45• “Clear Faults After Replacement of Faulted Components on Server or CMM” on page 46• “Oracle ILOM Event Log” on page 47• “Syslog Information” on page 48• “Collect SP Data to Diagnose System Problems” on page 49
Learn about managing system alerts in Oracle ILOM.	<ul style="list-style-type: none">• “Alert Management” on page 49• “Alert Management From the CLI” on page 53• “Alert Management From the Web Interface” on page 54• “Alert Management From an SNMP Host” on page 54

Related Information

- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage system components
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage system alerts
- *Oracle ILOM 3.0 Daily Management Web Procedures*, manage system components
- *Oracle ILOM 3.0 Daily Management Web Procedures*, manage system alerts
- *Oracle ILOM 3.0 Protocol Management Reference*, manage system components
- *Oracle ILOM 3.0 Protocol Management Reference*, manage system alerts

System Monitoring

The system monitoring features in Oracle ILOM enable you to easily determine the health of the system and to detect errors, at a glance, when they occur. For instance, in Oracle ILOM you can:

- View instantaneous sensor readings about system component temperatures, current, voltage, speed, and presence. For more information, see [“Sensor Readings” on page 41](#).
- Determine the state of indicators throughout the system. For more information, see [“System Indicators” on page 41](#).
- Monitor the state of system components. For more information, see [“Component Management” on page 42](#).
- Monitor the health of system components, as well as diagnose hardware failures, see [“Fault Management” on page 45](#).
- Clear faults after replacement of faulty components, see [“Clear Faults After Replacement of Faulted Components on Server or CMM” on page 46](#).
- Identify system errors and view event information in the Oracle ILOM event log. For more information, see [“Oracle ILOM Event Log” on page 47](#).
- Combine and view events from multiple instances in Oracle ILOM by sending Syslog information. For more information, see [“Syslog Information” on page 48](#).
- Collect data for use by Oracle Services personnel to diagnose system problems. For more information, see [“Collect SP Data to Diagnose System Problems” on page 49](#).

This topic contains the following information:

- [“Sensor Readings” on page 41](#)
- [“System Indicators” on page 41](#)
- [“Component Management” on page 42](#)
- [“Fault Management” on page 45](#)
- [“Clear Faults After Replacement of Faulted Components on Server or CMM” on page 46](#)
- [“Oracle ILOM Event Log” on page 47](#)
- [“Syslog Information” on page 48](#)
- [“Collect SP Data to Diagnose System Problems” on page 49](#)

Sensor Readings

All Oracle Sun server platforms are equipped with a number of sensors that measure voltages, temperatures, fan speeds, and other attributes about the system. Each sensor in Oracle ILOM contains nine properties describing various settings related to a sensor such as sensor type, sensor class, sensor value, as well as the sensor values for upper and lower thresholds.

Oracle ILOM regularly polls the sensors in the system and reports any events it encounters about sensor state changes or sensor threshold crossings to the Oracle ILOM event log. Additionally, if an alert rule was enabled in the system that matched the crossing threshold level, Oracle ILOM would automatically generate an alert message to the alert destination that you have defined.

You can view sensor readings from the Oracle ILOM web interface or CLI. For details, see “View Sensor Readings” in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

System Indicators

System indicator LEDs are generally illuminated on the system by Oracle ILOM based on the server platform policy. Typically the system indicator LEDs are illuminated by Oracle ILOM when any of the following conditions occur:

- Fault or error is detected on a component.
- Field-replacement unit (FRU) requires service.
- Hot-plug module is ready for removal.
- Activity is occurring on FRU or system.

You can view the states of system indicators from the Oracle ILOM web interface or the CLI. Additionally, in some instances, you might be able to modify the state of a system indicator. For details, see the section about View and Manage System Indicators in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Supported System Indicator States

Oracle ILOM supports the following system indicator states:

- **Off** – Normal operating status. Service is not required.
- **Steady On** – Component is ready for removal.

- **Slow Blink** – Component is changing state.
- **Fast Blink** – Helps locate a system in a data center.
- **Standby Blink** – Component is ready for activation, but is not operational at this time.

Types of System Indicator States

Oracle ILOM supports two types of system indicator states: *customer changeable* and *system assigned*.

- **Customer Changeable States** – Some system indicator LEDs in Oracle ILOM offer customer changeable states. Typically, these types of system indicators provide operational states of various system components. The type of states presented is determined by the system indicator. For example, depending on the system indicator, the following customer changeable states might be present:
 - **Off** – Normal operating status. Service is not required.
 - **Fast Blink** – Helps locate system in a data center.
- **System Assigned States** – System assigned indicators are *not* customer configurable. These types of system indicators provide read-only values about the operational state of a component. On most Oracle Sun server platforms, system assigned indicators are *Service Action Required LEDs*. These types of LEDs are typically illuminated when any of the following conditions are detected:
 - Fault or error is detected on a system component.
 - Hot-plug module is ready for removal.
 - Field-replacement unit (FRU) requires service.

Component Management

The Component Management features in Oracle ILOM enable you to monitor the state of various components that are installed on the server or managed by the Chassis Monitoring Module (CMM). For example, by using the Component Management features, you can:

- Identify the component name and type.
- Identify and change the component state (enabled or disabled).
- Identify the component's fault status and, if necessary, clear the fault.
- Prepare to install or remove a component.

- Filter the component management display by Fault Status, Component State, Hardware Type, and Ready to Remove Status. Or, create a Custom Filter to filter the component management display by Component or FRU Name, Component or FRU part number, Ready to Remove Status (Ready or Not Ready), and Fault Status (OK or Faulted).

Depending on the component type, you can view the component information or you can view and modify the state of component.

The Component Management features are supported in both the Oracle ILOM Web Interface and command-line interface (CLI) for x86 systems server SPs, SPARC systems server SPs, and CMMs. For detailed instructions for managing system components from the Oracle ILOM web interface or the CLI, see the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Oracle ILOM web interface examples of the Component Management features for a server SP and CMM are shown in the following figures.

FIGURE: Server SP Component Management Features in Web Interface

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

Overview
Components
Fault Management
Identification Information
Banner Messages
Session Timeout
Versions

Component Management

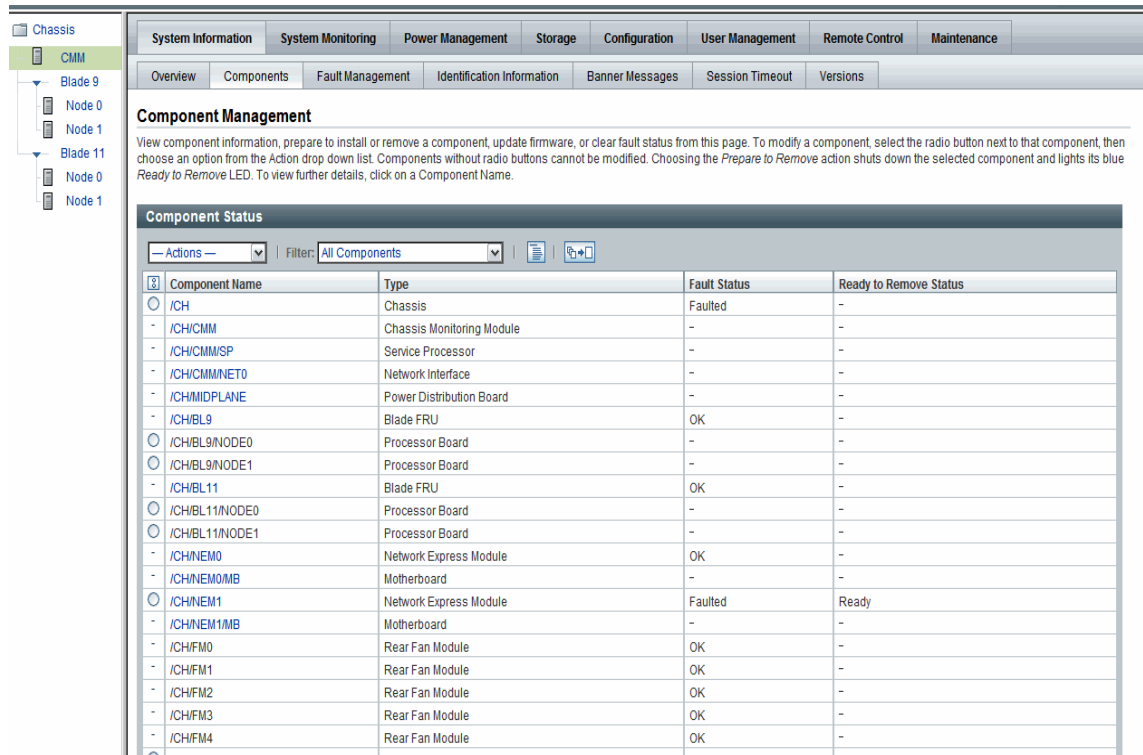
View component information, prepare to install or remove a component, change component state, or clear fault status from this page. To modify a component, select the radio button next to that component, then choose an option from the Action drop down list. Components without radio buttons cannot be modified. Choosing the *Prepare to Remove* action shuts down the selected component and lights its blue *Ready to Remove* LED. To view further details, click on a Component Name.

Component Status

-- Actions --
Filter: All Components

[?]	Component Name	Type	Component State	Fault Status	Ready to Remove Status
-	/SYS	Host System	-	Faulted	-
<input type="radio"/>	/SYSMB	Motherboard	-	Faulted	-
-	/SYSMB/SP	SP Board Module	-	OK	-
<input type="radio"/>	/SYSMB/GBE	Network Module	Enabled	-	-
<input type="radio"/>	/SYSMB/PCIE-SWITCH0	PCISwitch	Enabled	-	-
<input type="radio"/>	/SYSMB/PCIE-SWITCH1	PCISwitch	Enabled	-	-
<input type="radio"/>	/SYSMB/PCIE-SWITCH2	PCISwitch	Enabled	-	-
<input type="radio"/>	/SYSMB/PCIE-SWITCH3	PCISwitch	Enabled	-	-
<input type="radio"/>	/SYSMB/USB	USB Port	Enabled	-	-
<input type="radio"/>	/SYSMB/HBA	Disk Backplane	Enabled	-	-
<input type="radio"/>	/SYSMB/CPU0	CPU Board 0	-	Faulted	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/BR0/CH0/D0	DIMM	Enabled	Faulted	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/BR0/CH1/D0	DIMM	Enabled	Faulted	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/BR1/CH0/D0	DIMM	Enabled	Faulted	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/BR1/CH1/D0	DIMM	Enabled	Faulted	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/MCU0	Memory Controller	Enabled	-	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/MCU1	Memory Controller	Enabled	-	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/L2_BANK0	L2 Bank	Enabled	-	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/L2_BANK1	L2 Bank	Enabled	-	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/L2_BANK2	L2 Bank	Enabled	-	-
<input type="radio"/>	/SYSMB/CPU0/CMP0/L2_BANK3	L2 Bank	Enabled	-	-

FIGURE: CMM Component Management Features in Web Interface



Fault Management

Most Oracle Sun server platforms support the fault management software feature in Oracle ILOM. This feature enables you to proactively monitor the health of your system hardware, as well as diagnose hardware failures as they occur. In addition to monitoring the system hardware, the fault management software monitors environmental conditions and reports when the system's environment is outside acceptable parameters. Various sensors on the system components are continuously monitored. When a problem is detected, the fault management software automatically:

- Illuminates the Server Action Required LED on the faulted component.
- Updates the Oracle ILOM management interfaces to reflect the fault condition.
- Records information about the fault in the Oracle ILOM event log.

The type of system components and environmental conditions monitored by the fault management software are determined by the server platform. For more details about which components are monitored by the fault management software, consult your Sun server platform documentation.

Note – The Oracle ILOM fault management feature is currently available on all Sun server platforms, with the exception of the Sun Fire X4100 or X4200 series servers.

You can view the status of faulted components from the Oracle ILOM web interface or CLI. For details, see “View Fault Status” in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Clear Faults After Replacement of Faulted Components on Server or CMM

The Oracle ILOM-based service processor (SP) receives error telemetry about error events that occur within the major system components on the host (CPU, memory, and I/O hub) and the environmental subsystem within the chassis (such as fans, power supplies, and temperature). The components and conditions are then diagnosed as fault events and captured in the Oracle ILOM event log.

As of Oracle ILOM 3.0.3, the steps that are necessary to clear a fault are largely dependent on the type of server platform you are using (server module versus rackmount server). For example:

- Oracle ILOM-based faults that occur on a server module are NOT persistent once the server module has been properly prepared for removal and is physically removed from the chassis. Therefore, no service actions are required to clear the fault after the component is physically replaced. The fault message is captured in the Oracle ILOM event log for historical purposes.
- Oracle ILOM-based faults that occur on a rackmount server ARE persistent and might require service actions to clear the fault after the component is physically replaced, unless the component is a hot-swappable component (such as a fan or power supply). Hot-swappable components are platform-specific; therefore, refer to the platform documentation for a list of the hot-swappable components. The fault message is captured in the Oracle ILOM event log for historical purposes. On a rackmount server, you must manually clear the following faults after physically replacing the components, which are not hot-swappable:
 - CPU fault
 - DIMM (memory module) fault
 - PCI card fault

- Motherboard fault (if the motherboard is not being replaced)
- Oracle ILOM-based faults that occur on components installed in a chassis containing CMM(s) are automatically cleared by the Oracle ILOM CMM when the faulted component is replaced. However, if the chassis-level component is not hot-serviceable, then the fault needs to be manually cleared from the Oracle ILOM CMM.

In particular, the CMM automatically clears faults on the following chassis-level components after the faulted components are replaced:

- CMM fault
- Fan fault
- Power supply fault
- Network express module (NEM) fault
- PCI express module fault

Note – For more information about the Oracle ILOM fault management features offered on your system, refer to the procedures guides in the Oracle ILOM 3.0 Documentation Collection and the documentation provided with your Oracle server platform.

For instructions about clearing a fault using the Oracle ILOM CLI or web interface, see the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Oracle ILOM Event Log

The Oracle ILOM event log enables you to view information about any event that occurred on the system. Some of these events include Oracle ILOM configuration changes, software events, warnings, alerts, component failure, as well as IPMI, PET, and SNMP events. The type of events recorded in the Oracle ILOM event log is determined by the server platform. For information about which events are recorded in the Oracle ILOM event log, consult your Sun server platform documentation.

Event Log Time Stamps and Oracle ILOM Clock Settings

Oracle ILOM captures time stamps in the event log based on the host server UTC/GMT timezone. However, if you view the event log from a client system that is located in a different timezone, the time stamps are automatically adjusted to the timezone of the client system. Therefore, a single event in the Oracle ILOM event log might appear with two timestamps.

In Oracle ILOM, you can choose to manually configure the Oracle ILOM clock based on the UTC/GMT timezone of the host server, or you can choose to synchronize the Oracle ILOM clock with other systems on your network by configuring the Oracle ILOM clock with an NTP server IP address.

Manage Event Log and Time Stamps From CLI, Web, or SNMP Host

You can view and manage the event log and time stamps in Oracle ILOM from the CLI, web interface, or an SNMP host. For details, see “Configure Clock Settings” and “Filter Event Log Output” in the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Syslog Information

Syslog is a standard logging utility used in many environments. Syslog defines a common set of features for logging events and also a protocol for transmitting events to a remote log host. You can use syslog to combine events from multiple instances of Oracle ILOM within a single place. The log entry contains all the same information that you would see in the local Oracle ILOM event log, including class, type, severity, and description.

For information about configuring Oracle ILOM to send syslog to one or two IP addresses, see “Configure Remote Syslog Receiver IP Addresses” in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Protocol Management Guide*

Collect SP Data to Diagnose System Problems

The Oracle ILOM Service Snapshot utility enables you to produce a snapshot of the SP at any instant in time. You can run the utility from the Oracle ILOM CLI or the web interface. For more information about collecting SP data to diagnose system problems, refer the *Oracle ILOM 3.0 Maintenance and Diagnostics CLI and Web Guide*.

Alert Management

Oracle ILOM supports alerts in the form of IPMI PET alerts, SNMP Trap alerts, and Email Notification alerts. Alerts provide advance warning of possible system failures. Alert configuration is available from the Oracle ILOM SP on your server.

Each Sun server platform is equipped with a number of sensors that measure voltages, temperatures, and other service-related attributes about the system. Oracle ILOM automatically polls these sensors and posts any events crossing a threshold to an Oracle ILOM event log, as well as generates alert message(s) to one or more customer-specified alert destinations. The alert destination specified must support the receipt of the alert message (IPMI PET or SNMP). If the alert destination does not support the receipt of the alert message, the alert recipient will be unable to decode the alert message.



Caution – Oracle ILOM tags all events or actions with LocalTime=GMT (or UTC). Browser clients show these events in LocalTime. This can cause apparent discrepancies in the event log. When an event occurs in Oracle ILOM, the event log shows it in UTC, but a client would show it in LocalTime. For more information about Oracle ILOM timestamps and clock settings, see [“Event Log Time Stamps and Oracle ILOM Clock Settings”](#) on page 48.

Alert Rule Configuration

In Oracle ILOM you can configure up to 15 alert rules using the Oracle ILOM web interface or CLI. For each alert rule you configure in Oracle ILOM, you must define three or more properties about the alert depending on the alert type.

The *alert type* defines the messaging format and the method for sending and receiving an alert message. Oracle ILOM supports these three alert types:

- IPMI PET alerts
- SNMP Trap alerts

- Email Notification alerts

All Sun server platforms support all three alert types.

Alert Rule Property Definitions

Oracle ILOM offers the following property values for defining an alert rule:

- Alert Type
- Alert Level
- Alert Destination
- Alert Destination Port
- Email Custom Sender
- Email Message Prefix
- Email Class Filter
- Email Type Filter
- SNMP Version (SNMP Trap alerts only)
- SNMP Community Name or User Name (SNMP Trap alerts only)

For information about each of these property values, see [TABLE: Properties for Defining Alert Rules on page 51](#).

TABLE: Properties for Defining Alert Rules

Property Name	Requirement	Description
Alert Type	Mandatory	<p>The alert type property specifies the message format and the delivery method that Oracle ILOM will use when creating and sending the alert message. You can choose to configure one of the following alert types:</p> <ul style="list-style-type: none">• IPMI PET Alerts. IPMI Platform Event Trap (PET) alerts are supported on all Sun server platforms and CMMs. For each IPMI PET alert you configure in Oracle ILOM, you must specify an IP address for an alert destination and one of four supported alert levels. Note that the alert destination specified must support the receipt of IPMI PET messages. If the alert destination does not support the receipt of IPMI PET messages, the alert recipient will not be able to decode the alert message.• SNMP Trap Alerts. Oracle ILOM supports the generation of SNMP Trap alerts to a customer-specified IP destination. All destinations specified must support the receipt of SNMP Trap messages. Note that SNMP Trap alerts are supported on rackmounted servers and blade server modules. Filtering options for SNMP traps are not available.• Email Notification Alerts. Oracle ILOM supports the generation of Email Notification alerts to a customer-specified email address. To enable the Oracle ILOM client to generate Email Notification alerts, Oracle ILOM initially requires you to configure the name of the outgoing SMTP email server that would be sending the Email alert messages.
Alert Destination	Mandatory	<p>The alert destination property specifies where to send the alert message. The alert type determines which destination you can choose to send an alert message. For example, IPMI PET and SNMP Trap alerts must specify an IP address destination. Email Notification alerts must specify an email address. If the proper format is not entered for an alert destination, Oracle ILOM will report an error.</p>
Alert Destination Port	Optional	<p>The alert destination port only applies when the alert type is an SNMP Trap. The destination port property specifies the UDP port to which SNMP Trap alerts are sent.</p>

TABLE: Properties for Defining Alert Rules

Property Name	Requirement	Description
Alert Level	Mandatory	<p>Alert levels act as a filter mechanism to ensure alert recipients only receive the alert messages that they are most interested in receiving. Each time you define an alert rule in Oracle ILOM, you must specify an alert level.</p> <p>The alert level determines which events generate an alert. The lowest level alert generates alerts for that level and for all alert levels above it.</p> <p>Oracle ILOM offers the following alert levels with Minor being the lowest alert offered:</p> <ul style="list-style-type: none"> • Minor. This alert level generates alerts for informational events, lower and upper non-critical events, upper and lower critical events, and, upper and lower non-recoverable events. • Major. This alert level generates alerts for upper and lower non-critical events, upper and lower critical events, and, upper and lower non-recoverable events. • Critical. This alert level generates alerts for upper and lower critical events and upper and lower non-recoverable events. • Down. This alert level generates alerts for only upper non-recoverable and lower non-recoverable events. • Disabled. Disables the alert. Oracle ILOM will not generate an alert message. All the alert levels will enable the sending of a alert with the exception of Disabled. <p>Important - Oracle ILOM supports alert level filtering for all IPMI traps and Email Notification traps. Oracle ILOM does not support alert level filtering for SNMP traps. To enable the sending of an SNMP trap (but not filter the SNMP trap by alert level) you can choose anyone of the following options: <i>Minor</i>, <i>Major</i>, <i>Critical</i>, or <i>Down</i>. To disable the sending of an SNMP trap, you must choose the <i>Disabled</i> option.</p>
Email Custom Sender	Optional	<p>The email custom sender property applies only when the alert type is an email alert. You can use the <code>email_custom_sender</code> property to override the format of the "from" address. You can use either one of these substitution strings: <code><IPADDRESS></code> or <code><HOSTNAME></code>; for example, <code>alert@[<IPADDRESS>]</code>. Once this property is set, this value will override any SMTP custom sender information.</p>
Email Message Prefix	Optional	<p>The email message prefix property applies only when the alert type is an email alert. You can use the <code>email_message_prefix</code> property to prepend information to the message content.</p>
Event Class Filter	Optional	<p>The event class filter property applies only when the alert type is an email alert. The default setting is to send every Oracle ILOM event as an email alert. You can use the <code>event_class_filter</code> property to filter out all information except the selected event class. You can use "" (empty double quotes) to clear the filter and send information about all classes.</p>

TABLE: Properties for Defining Alert Rules

Property Name	Requirement	Description
Event Type Filter	Optional	The event type filter property applies only when the alert type is an email alert. You can use the <code>event_type_filter</code> property to filter out all information except the event type. You can use "" (empty double quotes) to clear the filter and send information about all event types.
SNMP Version	Optional	The SNMP version property enables you to specify which version of an SNMP trap that you are sending. You can choose to specify: 1, 2c, or 3. This property value only applies to SNMP Trap alerts.
SNMP Community Name or User Name	Optional	The SNMP community name or user name property enables you to specify the community string or SNMP v3 user name used in the SNMP Trap alert. <ul style="list-style-type: none">• For SNMP v1 or v2c, you can choose to specify a community name value for an SNMP alert.• For SNMP v3, you can choose to specify a user name value for an SNMP alert. <p>Note - If you choose to specify an SNMP v3 user name value, you must define this user in Oracle ILOM as an SNMP user. If you do not define this user as an SNMP user, the trap receiver will not be able to decode the SNMP Trap alert. For more information about defining an SNMP user in Oracle ILOM, see the <i>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide</i>, or the <i>Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide</i>.</p>

Alert Management From the CLI

You can enable, modify, or disable any alert rule configuration in Oracle ILOM from the command-line interface (CLI). All 15 alert rule configurations defined in Oracle ILOM are disabled by default. To enable alert rule configurations in Oracle ILOM, you must set values for the following properties: alert type, alert level, and alert destination.

You can also generate test alerts to any enabled alert rule configuration in Oracle ILOM from the CLI. This test alert feature enables you to verify that the alert recipient(s) specified in an enabled alert rule configuration receives the alert message.

For additional information about how to manage alerts using the Oracle ILOM CLI, see "Managing System Alerts" in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Alert Management From the Web Interface

You can enable, modify, or disable any alert rule configuration in Oracle ILOM from the Alert Settings web interface page. All 15 alert rule configurations presented on this page are disabled by default. The Actions drop-down list box on the page enables you to edit the properties associated with an alert rule. To enable an alert rule on this page, you must define an alert type, alert level, and a valid alert destination.

The Alert Settings page also presents a Send Test Alert button. This test alert feature enables you to verify that each alert recipient specified in an enabled alert rule receives an alert message.

FIGURE: Alert Settings Page

Alert Settings

This shows the table of configured alerts. To send a test alert to each of the configured alert destinations, click the *Send Test Alerts* button. IPMI Platform Event Traps (PETs), Email Alerts and SNMP Traps are supported. Select a radio button, then select Edit from the Actions drop down list to configure an alert. You can configure up to 15 alerts.

Send Test Alerts

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

For additional information about how to manage alerts using the Oracle ILOM web interface, see “Managing System Alerts” in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Alert Management From an SNMP Host

You can use the `get` and `set` commands to view and configure alert rule configurations using an SNMP host.

Before you can use SNMP to view and configure Oracle ILOM settings, you must configure SNMP. For more information about how to use SNMP to manage system alerts, see “Managing System Alerts” in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide*.

Storage Monitoring and Zone Management

Description	Links
Learn about storage monitoring for HDDs and RAID controller.	<ul style="list-style-type: none">• “Storage Monitoring for HDDs and RAID Controllers” on page 57• “CLI Storage Properties Shown for HDDs and RAID Controllers” on page 58• “Monitoring Storage Components Using the CLI” on page 61• “Monitoring Storage Components Using the Web Interface” on page 61
Learn about the CMM Zone Management feature.	<ul style="list-style-type: none">• “CMM Zone Management Feature” on page 66

Related Information

- *Oracle ILOM 3.0 Daily Management CLI Procedures*, monitor storage components
- *Oracle ILOM 3.0 Daily Management Web Procedures*, monitor storage components
- *Oracle ILOM 3.0 CMM Administration*, using Sun Blade Zone Manager

Storage Monitoring for HDDs and RAID Controllers

As of Oracle ILOM 3.0.6, Oracle ILOM supports additional storage monitoring functions for viewing and monitoring storage details that are associated with system hard disk drives (HDDs) and RAID controllers. These enhanced storage property details are available in Oracle ILOM from the CLI (as of Oracle ILOM 3.0.6) and the web interface (as of Oracle ILOM 3.0.8).

Note – Some Oracle Sun servers might not enable support for the storage monitoring functions that are described in this chapter. To determine whether storage monitoring support on your server has been enabled, see the Oracle ILOM Supplement guide for your server.

For Oracle Sun servers supporting the Storage Monitoring feature in Oracle 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).

Topics in this section include:

- [“CLI Storage Properties Shown for HDDs and RAID Controllers” on page 58](#)
- [“Monitoring Storage Components Using the CLI” on page 61](#)
- [“Monitoring Storage Components Using the Web Interface” on page 61](#)

CLI Storage Properties Shown for HDDs and RAID Controllers

Using the Oracle ILOM CLI, you can view the following properties ([TABLE: Storage Properties Shown for HDDs and RAID Controllers on page 58](#)) that are associated with your system server HDDs and RAID controller options.

Note – The storage properties appearing in [TABLE: Storage Properties Shown for HDDs and RAID Controllers on page 58](#) might not be available for all storage configurations.

TABLE: Storage Properties Shown for HDDs and RAID Controllers

HDD Storage Properties (shown in Oracle ILOM CLI under /SYS)

• Disk type (SATA or SAS)	• OK to remove status	• HBA ID for controller
• FRU type (hard disk)	• Service fault state	• HBA ID for disk
• FRU name	• Present device state	• RAID status (online, offline, failed, missing, and so on)
• FRU part number	• Disk capacity	• RAID dedicated hot-spare (for disk)

TABLE: Storage Properties Shown for HDDs and RAID Controllers (Continued)

• FRU serial number	• Device name	• RAID global hot-spare (disk group)
• FRU manufacturer	• World Wide Name (WWN)	• RAID ID list that is applicable to the HDD
• FRU version	• FRU description	

RAID Controller Properties (shown in Oracle ILOM CLI under /STORAGE/raid)

• FRU manufacturer	• PCI subdevice	• Maximum global hot spares (allowed number of global hot spares for controller)
• FRU model	• RAID levels supported	• Minimum stripe size (supported size in kilobytes)
• PCI vendor ID	• Maximum disks (allowed disks for controller)	• Maximum stripe size (supported size in kilobytes)
• PCI device ID	• Maximum RAIDs (allowed logical volumes for controller)	
• PCI subvendor ID	• Maximum hot spares (allowed dedicated hot spares for single RAID)	

RAID Controller Disk Properties (shown in Oracle ILOM CLI under /STORAGE/raid)

• FRU name	• FRU version	• World Wide Name (WWN)
• FRU part number	• RAID status (offline, online, failed, missing, initializing)	• Dedicated hot spare (for disk)
• FRU serial number	• Disk capacity (supported size in byte)	• Global hot spare (for disk group)
• FRU manufacturer	• Device name	• RAID IDs (list for this device)
• FRU description	• Disk type (SAS or SATA known by host operating system)	• System drive slot (corresponding internal hard drive NAC name for RAID)

TABLE: Storage Properties Shown for HDDs and RAID Controllers *(Continued)*

RAID Controller Volume Properties (shown in Oracle ILOM CLI under /STORAGE/raid)

- RAID level
 - Mounted status
 - Stripe size
 - RAID volume status (OK, degraded, failed, missing)
 - Device name, known by host operating system
 - Targets for child member of RAID ID
 - Disk capacity
 - Resync status
-

RAID Status Definitions for Physical and Logical Drives

When a physical disk is configured as part of a volume and is attached to a powered-on controller, Oracle ILOM reports one of the following status values for configured physical ([TABLE: RAID Status Definitions for Physical RAID Disks on page 60](#)) and logical ([TABLE: Status Definitions for Logical RAID Volumes on page 61](#)) drives.

TABLE: RAID Status Definitions for Physical RAID Disks

Physical RAID Disk ID Status

OK	The disk is online.
Offline	The disk is offline per host request or for another reason such as disk is not compatible for use in volume.
Failed	The disk has failed.
Initializing	The disk is being initialized or rebuilt.
Missing	The disk is missing or not responding.
Unknown	The disk is not recognized.

TABLE: Status Definitions for Logical RAID Volumes

Logical RAID Volume Status	
OK	The volume is running at optimal level.
Degraded	The volume is running in degraded mode. An additional disk loss could result in permanent data loss.
Failed	The volume has too many failed disks and is not running.
Missing	The volume is not found or not available.
Unknown	The volume is not recognized or is not defined.

Monitoring Storage Components Using the CLI

To view and monitor storage details related to the HDDs and RAID controllers that are configured on your system, log in to the Oracle ILOM CLI and drill down the following target properties under:

- `/SYS/` to show details for HDDs

or

- `/STORAGE/raid` to show details for a RAID disk controller

For CLI procedures about how to view and monitor storage properties in Oracle ILOM, see the section about Viewing and Monitoring Storage Components in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

Monitoring Storage Components Using the Web Interface

To view and monitor storage details related to the HDDs and RAID controllers that are configured on your system, log in to the Oracle ILOM web interface and drill-down to the web interface Storage --> RAID tabs. From the RAID tab, you can view and monitor details about:

- Raid controllers (Controller tab) – see [“RAID Controllers Tab Details”](#) on page 62.
- Disks attached to RAID controllers (Disk tab) – see [“Disks Attached to RAID Controllers Details”](#) on page 63.
- RAID controller volume details (Volumes tab) – see [“RAID Controller Volume Details”](#) on page 65.

RAID Controllers Tab Details

From the Storage --> RAID --> Controller tab in Oracle ILOM, you can access configuration information about each RAID controller installed on your system. This information includes:

- RAID controller configuration details that describe the RAID levels, maximum number of disks, and the maximum number of RAID configurations that can be configured on each installed RAID controller. For example, see [FIGURE: RAID Controller Configuration Details on page 62](#).
- RAID controller FRU properties and values for each installed RAID controller. For example, see [FIGURE: RAID Controller FRU Properties and Values on page 63](#).
- RAID controller topology details that display information about attached disks, configured RAID volumes, and disks that are part of a RAID. For example, see [FIGURE: RAID Controller Topology Details on page 63](#).

FIGURE: RAID Controller Configuration Details

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

Controller Topology

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

FIGURE: RAID Controller FRU Properties and Values

controller@0d:00.0	
Property	Value
fru_manufacturer	LSI Logic
fru_model	0x0058
pci_vendor_id	0x00001000
pci_device_id	0x00000058
pci_subvendor_id	0x00001000
pci_subdevice_id	0x00003150
raid_levels	0, 1, 1E
max_disks	63
max_raids	2
max_hot_spare	0
max_global_hot_spare	2
min_stripe_size	0
max_stripe_size	0

FIGURE: RAID Controller Topology Details

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

Disks Attached to RAID Controllers Details

From the Storage --> RAID --> Disks tab in Oracle ILOM, you can access configuration information about the disks that are attached to your RAID controllers. This information includes:

- Disk configuration details for each disk attached to a RAID controller. These details include the disk name, status, serial number, capacity, and device name. For example, see [FIGURE: Disk Details - Attached to RAID Controller on page 64](#).

- Disk FRU properties and values for each disk attached to a RAID controller. For example, see [FIGURE: Disk FRU Properties and Values](#) on page 64.

FIGURE: Disk Details - Attached to RAID Controller

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

FIGURE: Disk FRU Properties and Values

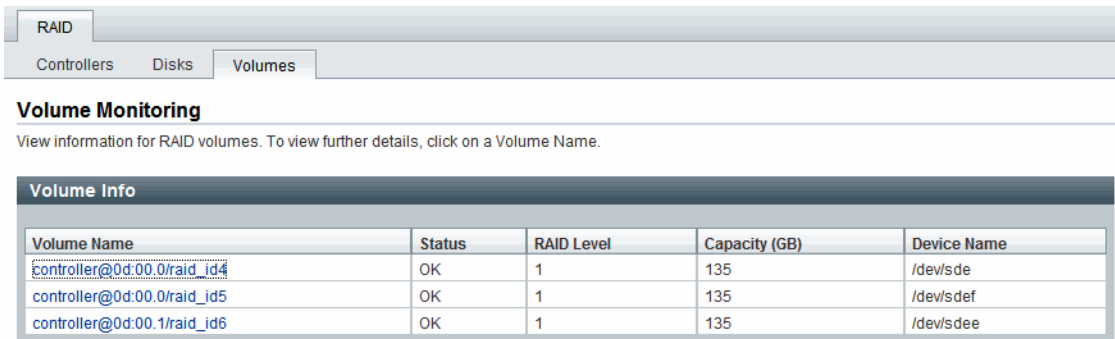
controller@0d:00.0/disk_id0	
Property	Value
fru_manufacturer	SEAGATE
fru_serial_number	0998SX6X 3NM8SX6X
fru_part_number	ST914602SSUN146G
fru_version	0603
capacity	136
device_name	/dev/sda
disk_type	sas
system_drive_slot	/SYS/DBP/HDD0

RAID Controller Volume Details

From the Storage --> RAID --> Volume tab in Oracle ILOM, you can access configuration information about the RAID volumes that are configured on RAID controllers. This information includes:

- Volume configuration details for each volume configured on a RAID controller. These details include the volume name, status, RAID level, capacity, and device name. For example, see [FIGURE: RAID Volume Configuration Details on page 65](#).
- Volume properties and values for each volume configured on a RAID controller. For example, see [FIGURE: RAID Volume Properties and Values on page 65](#).

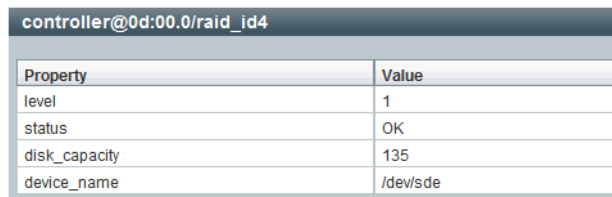
FIGURE: RAID Volume Configuration Details



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

FIGURE: RAID Volume Properties and Values

View volume information.



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

For web procedures about how to view and monitor storage properties in Oracle ILOM, see the section about Viewing and Monitoring Storage Components in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

CMM Zone Management Feature

As of Oracle ILOM 3.0.10, a new zoning management feature is available on the CMM for SAS-2 storage devices that are installed in Oracle Sun Blade 6000 or Sun Blade 6048 Modular Systems.

For more information about how to manage SAS-2 chassis storage devices from Oracle ILOM, see the section about Zone management in the *Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems* (820-0052).

Power Monitoring and Management of Hardware Interfaces

Description	Links
Identify Power Monitoring and Management feature updates per Oracle ILOM firmware point release.	<ul style="list-style-type: none">• “Summary of Power Management Feature Updates” on page 68
Become familiar with the power management terminology.	<ul style="list-style-type: none">• “Power Monitoring Terminology” on page 70
Learn about Oracle ILOM’s real-time power monitoring and management features.	<ul style="list-style-type: none">• “System Power Consumption Metrics” on page 73• “Power Policy Settings for Managing Server Power Usage” on page 80• “Power Usage Statistics and History Metrics for Server SP and CMM” on page 83• “Power Consumption Threshold Notifications as of Oracle ILOM 3.0.4” on page 89• “Component Allocation Distribution as of Oracle ILOM 3.0.6 for Server SP and CMM” on page 90• “Power Budget as of Oracle ILOM 3.0.6 for Server SPs” on page 99• “Power Supply Redundancy for CMM Systems as of Oracle ILOM 3.0.6” on page 105• “Platform-Specific CMM Power Metrics as of Oracle ILOM 3.0.6” on page 106

Related Information

- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage power consumption
- *Oracle ILOM 3.0 Daily Management Web Procedures*, manage power consumption
- *Oracle ILOM 3.0 Protocol Management*, manage power consumption

Summary of Power Management Feature Updates

TABLE: Power Management Feature Updates per Oracle ILOM Firmware Point Release on page 68 identifies the common power management feature enhancements and documentation updates made since Oracle ILOM 3.0.

TABLE: Power Management Feature Updates per Oracle ILOM Firmware Point Release

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Conceptual Information, See:
Monitor Power Consumption Metrics	Oracle ILOM 3.0	<ul style="list-style-type: none"> • New terms and definitions explained 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"> • “Power Monitoring Terminology” on page 70 • “Web Interface Power Consumption Metrics as of Oracle ILOM 3.0” on page 74
Configure Power Policy Properties	Oracle 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"> • “Power Policy Settings as of Oracle ILOM 3.0” on page 80
Monitor Power Consumption History	Oracle ILOM 3.0.3	<ul style="list-style-type: none"> • New power consumption history metrics explained. • New CLI and web procedures added for monitoring power consumption. 	<ul style="list-style-type: none"> • “Power Usage Statistics and History Metrics for Server SP and CMM” on page 83
Web Interface Layout Update for Server Power Management	Oracle ILOM 3.0.4	<ul style="list-style-type: none"> • New top level tab added to Oracle ILOM web interface for Power Management -->Consumption page and History page • Updated procedures for Monitoring Power Consumption and History. 	<ul style="list-style-type: none"> • “Web Interface Server and CMM Power Consumption Metrics As of Oracle ILOM 3.0.4” on page 76
Configure Power Consumption Notification Thresholds	Oracle ILOM 3.0.4	<ul style="list-style-type: none"> • New power consumption notification threshold settings explained. • New CLI and web procedures added for configuring the power consumption thresholds. 	<ul style="list-style-type: none"> • “Power Consumption Threshold Notifications as of Oracle ILOM 3.0.4” on page 89

TABLE: Power Management Feature Updates per Oracle ILOM Firmware Point Release *(Continued)*

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Conceptual Information, See:
Monitor Allocation Power Distribution Metrics	Oracle ILOM 3.0.6	<ul style="list-style-type: none">• New component allocation distribution metrics explained.• New CLI and web procedures added for monitoring power allocations.• New CLI and web procedures for configuring permitted power for blade slots.	<ul style="list-style-type: none">• “Component Allocation Distribution as of Oracle ILOM 3.0.6 for Server SP and CMM” on page 90
Configure Power Budget Properties	Oracle ILOM 3.0.6	<ul style="list-style-type: none">• New power budget properties explained.• New CLI and web procedures added for configuring power budget properties.	<ul style="list-style-type: none">• “Power Budget as of Oracle ILOM 3.0.6 for Server SPs” on page 99
Configure Power Supply Redundancy Properties for CMM Systems	Oracle ILOM 3.0.6	<ul style="list-style-type: none">• New power supply redundancy properties for CMM systems explained.• New CLI and web procedures added for configuring power supply redundancy properties on CMM systems.	<ul style="list-style-type: none">• “Power Supply Redundancy for CMM Systems as of Oracle ILOM 3.0.6” on page 105
Monitor Advanced Power Metrics for Server Module from CMM	Oracle ILOM 3.0.6	<ul style="list-style-type: none">• New CMM advanced power metrics explained for server modules.	<ul style="list-style-type: none">• “Platform-Specific CMM Power Metrics as of Oracle ILOM 3.0.6” on page 106
Server Power Consumption Tab Properties Renamed	Oracle ILOM 3.0.8	<ul style="list-style-type: none">• Revised Oracle ILOM web interface Power Consumption tab properties explained for server SPs.	<ul style="list-style-type: none">• “Web Enhancements for Server SP Power Consumption Metrics As of 3.0.8” on page 77
Server Power Allocation Tab Replaces Distribution Tab	Oracle ILOM 3.0.8	<ul style="list-style-type: none">• Oracle ILOM web Allocation tab replaces Distribution tab for server SPs.• New web procedure for viewing server power allocation properties	<ul style="list-style-type: none">• “Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.8 (Server SP)” on page 95
Server Limit Tab Replaces Budget Tab	Oracle ILOM 3.0.8	<ul style="list-style-type: none">• Oracle ILOM web Limit tab replaces Budget tab for server SPs.• New web procedure for configuring power limit properties	<ul style="list-style-type: none">• “Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.8 (Server SP)” on page 95

TABLE: Power Management Feature Updates per Oracle ILOM Firmware Point Release *(Continued)*

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Conceptual Information, See:
Web Interface Layout Update for CMM Power Management	Oracle ILOM 3.0.10	<ul style="list-style-type: none"> • New top level tab added to Oracle ILOM web interface for Power Management • Revised Oracle ILOM web Power Consumption tab properties for CMMs explained. • Oracle ILOM web Allocation tab replaces Distribution tab for CMMs. • Power Management Metrics tab removed from CMM Oracle ILOM web interface • Updated web procedure for configuring a grant limit for blade slots (previously known as allocatable power) 	<ul style="list-style-type: none"> • “Web Enhancements for CMM Power Consumption Metrics As of 3.0.10” on page 78 • “Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.10 (CMM)” on page 96 • “Platform-Specific CMM Power Metrics as of Oracle ILOM 3.0.6” on page 106
CLI Property Update for CMM Power Management	Oracle ILOM 3.0.10	<ul style="list-style-type: none"> • Revised CLI properties under the blade slot target explained. • Updated CLI procedure for configuring granted power or reserved power for blade slots • Updated CLI procedure for viewing power or grant limit for blade • Updated CLI procedure for configuring grant limit for blade 	<ul style="list-style-type: none"> • “Revised CLI Power Allocation Properties as of Oracle ILOM 3.0.10” on page 98
Web Power Management Statistics tab	Oracle ILOM 3.0.14	<ul style="list-style-type: none"> • Power statistics previously available on the History tab have been moved to the Power Management -->Statistic tab. 	<ul style="list-style-type: none"> • “Power Usage Statistics and History Web Enhancements as of Oracle ILOM 3.0.4” on page 86

Power Monitoring Terminology

TABLE: Power Monitoring Terminology as of Oracle ILOM 3.0.3 on page 71 identifies the initial power monitoring terminology and definitions as of Oracle ILOM 3.0.3.

TABLE: Power Monitoring Terminology as of Oracle ILOM 3.0.3

Terms	Definition
Real-time power monitoring hardware interfaces	Power monitoring hardware interfaces enable real-time real time means that the service processor (SP) or individual power supply can be polled at any instance to retrieve and report “live” data to within one second accuracy
Power Consumption	Power consumption that is reported in Oracle ILOM includes input and output power. <ul style="list-style-type: none"> • Input Power <i>Input power</i> is the power that is pulled into the system’s power supplies from an external source. • Output Power <i>Output power</i> is the amount of power provided from the power supply to the system components.
Total Power Consumption	The <i>total power consumption</i> that is reported in Oracle ILOM is dependent on the hardware configuration: rackmount server, server module, or chassis monitoring module. <ul style="list-style-type: none"> • Rackmount Server Total Power Consumption The <i>rackmount server total power consumption</i> is the input power consumed by the server. • Server Module Total Power Consumption The <i>server module (blade) total power consumption</i> is the input power consumed only by the blade and not including any power consumed by shared components. • CMM Total Power Consumption The <i>CMM total power consumption</i> is the input power consumed by the entire chassis or shelf.
Power Consumption Monitoring Properties	<i>Power consumption monitoring properties</i> include: maximum power, actual power, available power, and permitted power. <p>Note - Some Oracle server platforms might not provide the power management metrics for maximum power, actual power, available power and permitted power.</p> <ul style="list-style-type: none"> • Hardware Maximum Power Consumption Property <i>Hardware maximum power</i> identifies the maximum input power that a system is capable of consuming at any instant given the hardware configuration of the system. Therefore, the hardware configuration maximum power is the sum of the maximum power that each processor, I/O module, memory module, fan, and so forth is capable of consuming. <p>Note - The hardware maximum power consumption metric is not available from the Oracle ILOM web interface.</p>

TABLE: Power Monitoring Terminology as of Oracle ILOM 3.0.3 (*Continued*)

Terms	Definition
<ul style="list-style-type: none">• Actual Power Property	<p><i>Actual Power</i> represents the consumed power for the rackmount server or chassis system. On a chassis monitoring module, this is the input power consumed by the entire chassis or shelf (all blades, NEMS, fans, and so forth).</p> <p>Note - The Actual Power value is made available via the <code>/SYS/VPS</code> sensor.</p>
<ul style="list-style-type: none">• Available Power Property	<p><i>Available power</i> is the maximum power that the power supplies in the system can draw from an external source, for example:</p> <ul style="list-style-type: none">• For rackmount servers, the available power value represents the maximum input power that the power supplies are cable of consuming.• For chassis systems, this available power value represents the available amount of power guaranteed to the server module (blade) by the chassis.
<ul style="list-style-type: none">• Permitted Power Property <p>or</p> <ul style="list-style-type: none">• Peak Permitted Property	<p>The <i>Permitted Power or Peak Permitted</i> (see note below) is the maximum power consumption guaranteed, for example:</p> <ul style="list-style-type: none">• For rackmount servers, the permitted power represents the maximum input power that the server guarantees it will consume at any instant.• For chassis systems, the permitted power represents the maximum power a server module guarantees it will consume at any instant. <p>Note - The <i>Permitted Power</i> property on the server SP was renamed to <i>Peak Permitted</i> as of Oracle ILOM 3.0.8. The <i>Permitted Power</i> property on the CMM was renamed to <i>Peak Permitted</i> as of Oracle ILOM 3.0.10.</p>
<ul style="list-style-type: none">• Additional platform-specific power management metrics	<p>Some servers might provide additional platform-specific power metrics under the <code>/SP/powermgmt/advanced</code> mode in the CLI or the Advanced Power Metrics table in the system Monitoring --> Power Management page in the web interface. Each advanced power metric includes a name, a unit, and a value.</p> <p>For additional information about platform-specific power management information, see the Oracle ILOM Supplement guide or the administrator guide that was provided with your server system.</p>

For information about how to view the power management metrics in Oracle ILOM using the CLI or web interface, see the section about Monitoring the Power Consumption Interfaces in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)

Real-Time Power Monitoring and Management Features

For details, about using Oracle ILOM's real-time power monitoring and management features see these topics:

- [“System Power Consumption Metrics” on page 73](#)
- [“Power Policy Settings for Managing Server Power Usage” on page 80](#)
- [“Power Usage Statistics and History Metrics for Server SP and CMM” on page 83](#)
- [“Power Consumption Threshold Notifications as of Oracle ILOM 3.0.4” on page 89](#)
- [“Component Allocation Distribution as of Oracle ILOM 3.0.6 for Server SP and CMM” on page 90](#)
- [“Power Budget as of Oracle ILOM 3.0.6 for Server SPs” on page 99](#)
- [“Power Supply Redundancy for CMM Systems as of Oracle ILOM 3.0.6” on page 105](#)
- [“Platform-Specific CMM Power Metrics as of Oracle ILOM 3.0.6” on page 106](#)

System Power Consumption Metrics

As of Oracle ILOM 3.0, you can view the server SP and CMM power consumption metrics using the Oracle ILOM CLI or web interface.

Since Oracle ILOM 3.0, web enhancements for the Power Consumption metrics have been made in Oracle ILOM 3.0.4, 3.0.8, and 3.0.10. The CLI power consumption metrics targets and properties have not changed since Oracle ILOM 3.0.

For information about how to access the power consumption metrics in Oracle ILOM, as well as updates made to the power consumption web interface since Oracle ILOM 3.0, see the following topics:

Oracle ILOM Interface	Platform Hardware	As of Oracle ILOM Firmware	Power Consumption Topic
Web	Server SP and CMM	Oracle ILOM 3.0	“Web Interface Power Usage Statistics and History Metrics” on page 84
CLI	Server SP and CMM	Oracle ILOM 3.0	“CLI Power Consumption Metrics as of Oracle ILOM 3.0” on page 75
Web	Server SP and CMM	Oracle ILOM 3.0.4	“Web Interface Server and CMM Power Consumption Metrics As of Oracle ILOM 3.0.4” on page 76
Web	Server SP	Oracle ILOM 3.0.8	“Web Enhancements for Server SP Power Consumption Metrics As of 3.0.8” on page 77
Web	CMM	Oracle ILOM 3.0.10	“Web Enhancements for CMM Power Consumption Metrics As of 3.0.10” on page 78
CLI	CMM	Oracle ILOM 3.0.10	“Revised CLI Power Allocation Properties as of Oracle ILOM 3.0.10” on page 98

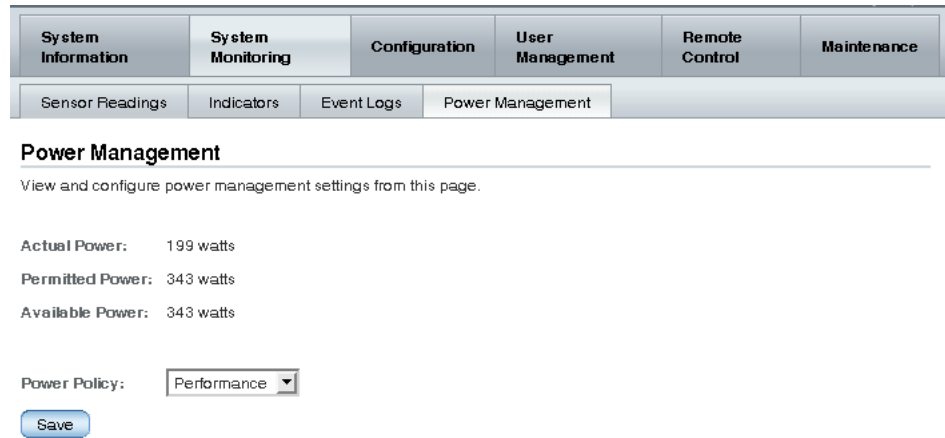
Note – The ability to monitor and provide the power consumption metrics in Oracle ILOM varies depending on the platform server implementation of this feature. For information about hardware platform-specific power consumption metrics provided for your server, see the Oracle ILOM Supplement Guide or administration guide provided with your system.

Web Interface Power Consumption Metrics as of Oracle ILOM 3.0

As of Oracle ILOM 3.0, you can control the power policy and view the power consumption metrics for a server SP or a CMM from the Power Management tab in the web interface.

The power consumption metrics (shown in [FIGURE: Power Management Web Interface Page as of Oracle ILOM 3.0. on page 75](#)) for Actual Power, Permitted Power and Available Power are defined in [TABLE: Power Monitoring Terminology as of Oracle ILOM 3.0.3 on page 71](#). For information describing the use of the Power Policy property, see [“Power Policy Settings for Managing Server Power Usage” on page 80](#).

FIGURE: Power Management Web Interface Page as of Oracle ILOM 3.0.



CLI Power Consumption Metrics as of Oracle ILOM 3.0

The following table identifies the server SP and CMM power consumption metric properties available from the Oracle ILOM CLI as of Oracle ILOM 3.0.

TABLE: CLI Power Consumption Properties

Power Consumption Property	Use the <code>show</code> command to view the power consumption property value, for example:
Total System Power Consumption	<code>show /SYS/VPS</code>
Actual Power Consumption	<code>show /SP/powermangement actual_power</code> Note - The actual power value returned is the same as the value returned by /SYS/VPS sensor.
Power Supply Consumption	<ul style="list-style-type: none"> For rackmount server power supply: <code>show /SYS/platform_path_to_powersupply/INPUT_POWER OUTPUT POWER</code> For CMM power supply: <code>show /CH/platform_path_to_powersupply/INPUT_POWER OUTPUT POWER</code>

TABLE: CLI Power Consumption Properties (*Continued*)

Power Consumption Property	Use the <code>show</code> command to view the power consumption property value, for example:
Actual Power	<ul style="list-style-type: none"> For rackmount servers: <code>show /SP/powermgmt available_power</code> For CMMs: <code>show /CMM/powermgmt available_power</code>
Maximum Hardware Power Consumption	<code>show /SP/powermgmt hwconfig_power</code>
Permitted Power Consumption	<ul style="list-style-type: none"> For rackmount servers: <code>show /SP/powermgmt permitted_power</code> For CMMs: <code>show /CMM/powermgmt permitted_power</code>

Web Interface Server and CMM Power Consumption Metrics As of Oracle ILOM 3.0.4

As of Oracle ILOM 3.0.4, the server SP and CMM power consumption metrics in the web interface have been moved to the Power Management --> Consumption page.

FIGURE: Power Consumption Page as of Oracle ILOM 3.0.4

The screenshot shows the Oracle ILOM 3.0.4 web interface. At the top, there is a navigation bar with tabs for System Information, System Monitoring, Power Management, Configuration, User Management, Remote Control, and Maintenance. The Power Management tab is selected, and within it, the Consumption sub-tab is active. Below the navigation bar, the page title is "Power Consumption". A descriptive text states: "View power consumption and configure notification thresholds from this page. An ILOM event will be generated when the actual power consumption level exceeds...". The main content area displays three power metrics: Actual Power (210 watts), Permitted Power (667 watts), and Available Power (1050 watts), each with a brief explanation. Below these metrics are two notification threshold settings, both with checkboxes for "Enabled" (currently unchecked) and input fields for "watts" (both set to 0). A "Save" button is located at the bottom left of the page.

A list of the server SP and CMM power consumption changes made in Oracle ILOM 3.0.4 are as follows:

- New properties for Notification Thresholds were added. For information about the Notification Threshold properties, see [“Power Consumption Threshold Notifications as of Oracle ILOM 3.0.4”](#) on page 89.
- The Power Policy property (shown in [FIGURE: Power Management Web Interface Page as of Oracle ILOM 3.0. on page 75](#)) was removed from the earlier version of the Power Management page. For more information about using the power policy property after Oracle ILOM 3.0.4, see [“Power Policy Settings for Managing Server Power Usage”](#) on page 80.
- The properties for *Actual Power*, *Permitted Power*, and *Available Power* remained unchanged. For more information about these properties, see [TABLE: Power Monitoring Terminology as of Oracle ILOM 3.0.3 on page 71](#).

Web Enhancements for Server SP Power Consumption Metrics As of 3.0.8

As of Oracle ILOM 3.0.8, some of the power consumption properties on the web interface for the server SP have changed. For more information about these property changes, see [TABLE: Consumption Tab Server SP Settings Changes in Oracle ILOM 3.0.8 on page 78](#).

FIGURE: Updated Power Management --> Consumption Tab - Oracle ILOM SP 3.0.8

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

Power Consumption

View actual system input power consumption, power consumption limit, and configure notification thresholds from this page. An ILOM event is generated when power consumption 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)

TABLE: Consumption Tab Server SP Settings Changes in Oracle ILOM 3.0.8

Consumption Tab Changes	Details
-Target -Limit (new property)	<p>A new read-only property for -Target -Limit is available on the Power Management --> Consumption tab as of Oracle ILOM 3.0.8.</p> <p>The -Target -Limit (shown in FIGURE: Updated Power Management --> Consumption Tab - Oracle ILOM SP 3.0.8 on page 77) property represents the power consumption limit value that was configured for the server.</p> <p>Note - The configuration options for the -Target -Limit property appear on the Power Management --> Limit tab. For more details about the -Target -Limit configuration options, see "Power Management --> Budget Tab Renamed to Limit Tab as of Oracle ILOM 3.0.8" on page 103.</p>
-Peak -Permitted (renamed property)	<p>The -Permitted -Power property on the Power Management --> Consumption tab in Oracle ILOM 3.0.4 (shown in FIGURE: Updated Power Management --> Consumption Tab - Oracle ILOM SP 3.0.8 on page 77) was renamed to -Peak -Permitted in Oracle ILOM 3.0.8.</p> <p>The -Peak -Permitted read-only property (shown in FIGURE: Updated Power Management --> Consumption Tab - Oracle ILOM SP 3.0.8 on page 77) represents the maximum power the system can consume.</p> <p>Note - For servers, the Peak Permitted value in Oracle ILOM is derived from the System Allocated power and the Target Limit. For more details, see "Advanced Server Power Budget Features as of Oracle ILOM 3.0.6" on page 101.</p>
-Allocated -Power (removed)	<p>The read-only property for -Allocated Power (shown in FIGURE: Power Consumption Page as of Oracle ILOM 3.0.4 on page 76) was removed from the Power Management --> Consumption tab as of Oracle ILOM 3.0.8 (shown in FIGURE: Power Consumption Page as of Oracle ILOM 3.0.4 on page 76).</p> <p>Note - In Oracle ILOM 3.0.8, you can view Allocated Power values for the system and for each component on the Power Allocation Plan page. For more details, see "Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.8 (Server SP)" on page 95.</p>

Web Enhancements for CMM Power Consumption Metrics As of 3.0.10

As of Oracle ILOM 3.0.10, some of the power consumption properties on the web interface for the CMM have changed. For more information about these property changes, see [TABLE: Consumption Tab CMM Settings Changes in Oracle ILOM 3.0.10 on page 79](#).

FIGURE: Updated Power Management --> Consumption Tab - Oracle ILOM CMM 3.0.10

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

Power Consumption

View the actual system input power consumption, peak permitted consumption, and configure notification thresholds. An ILOM event is generated when the actual consumption exceeds either threshold.

Actual Power: 1200 watts [Details...](#)
The input power the system is currently consuming.

Peak Permitted: 6400 watts (redundancy policy is applied)
Maximum power the system is permitted to consume.

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

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

TABLE: Consumption Tab CMM Settings Changes in Oracle ILOM 3.0.10

Consumption Tab Changes	Details
-Peak -Permitted (renamed property)	The -Permitted -Power property on the CMM Power Management --> Consumption tab was renamed to -Peak -Permitted in Oracle ILOM 3.0.10. The -Peak -Permitted read-only property (shown in FIGURE: Updated Power Management --> Consumption Tab - Oracle ILOM CMM 3.0.10 on page 79) represents the maximum power the system is permitted to use.
-Available Power (renamed property and moved)	The read-only property for -Available Power (previously available in Oracle ILOM 3.0.4) was removed from the CMM Power Management --> Consumption tab as of Oracle ILOM 3.0.10 (shown in FIGURE: Updated Power Management --> Consumption Tab - Oracle ILOM CMM 3.0.10 on page 79). The read-only property for Available Power was renamed to Grantable Power in Oracle ILOM 3.0.10 and moved to the Power Summary table on the Allocation tab. For more details, see “Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.10 (CMM)” on page 96.

Power Policy Settings for Managing Server Power Usage

To help manage the power usage of your system, Oracle ILOM supports the following Power policies:

- [“Power Policy Settings as of Oracle ILOM 3.0” on page 80](#)
- [“Power Policy Settings as of Oracle ILOM 3.0.4” on page 81](#)
- [“Power Capping Policy Settings as of Oracle ILOM 3.0.8” on page 81](#)

Power Policy Settings as of Oracle ILOM 3.0

As of Oracle ILOM 3.0, two Power Policy settings (shown in [FIGURE: Power Management Web Interface Page as of Oracle ILOM 3.0. on page 75](#)) are available from the Oracle ILOM CLI and web interface to help you manage the power usage on your system.

Note – The Power Policy feature was initially available on most x86 servers as of Oracle ILOM 3.0. As of Oracle ILOM 3.0.3, some SPARC platform servers supported this feature as well. To determine if your server supports a Power Policy feature, see the Oracle ILOM Supplement guide or administration guide provided for your server.

[TABLE: Power Policy Properties Defined as of Oracle ILOM 3.0 on page 80](#) defines the two Policy settings you can choose to configure from the Oracle ILOM CLI and web interface:

TABLE: Power Policy Properties Defined as of Oracle ILOM 3.0

Property	Description
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

For more details about how to access and configure the power policy settings in Oracle ILOM, see the section about Monitoring Power Consumption in one of the following guides:

- [Oracle Integrated Lights Out Manager \(ILOM\) 3.0 CLI Procedures Guide](#)
- [Oracle Integrated Lights Out Manager \(ILOM\) 3.0 Web Interface Procedures Guide](#)

- Oracle Integrated Lights Out Manager (ILOM) 3.0 Protocol Management Guide

Power Policy Settings as of Oracle ILOM 3.0.4

As of Oracle ILOM 3.0.4, the Power Policy settings in the Oracle ILOM interface have been changed as follows:

- The Power Management Power Policy properties available in the Oracle ILOM CLI or web interface (shown in [FIGURE: Power Management Web Interface Page as of Oracle ILOM 3.0. on page 75](#)) were removed for x86 server SPs as of Oracle ILOM 3.0.4.
- The Power Management Power Policy properties available in the Oracle ILOM web interface (shown in [FIGURE: Power Management Web Interface Page as of Oracle ILOM 3.0. on page 75](#)) for SPARC server supporting this feature have been moved to the Power Management -->Settings tab (shown in [FIGURE: Policy on Limit Tab for Some SPARC Servers as of Oracle ILOM 3.04. on page 81](#)). To verify if your SPARC system supports this feature, see the Oracle ILOM Supplement Guide or the administration guide supplied for your server.

FIGURE: Policy on Limit Tab for Some SPARC Servers as of Oracle ILOM 3.04.

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

Power Management Settings

View and configure the power policy from this page.

Power Policy:

Choices are:

- Performance: All components run at full speed/capacity.
- Elastic: Components are brought in to or out of a slower speed or a sleep state to match the system's utilization of those components.

Power Capping Policy Settings as of Oracle ILOM 3.0.8

As of Oracle ILOM 3.0.8, advanced policy settings (shown in [FIGURE: Advanced Power Policy Appear on Limit Tab as of Oracle ILOM 3.0.8 on page 83](#)) for power capping were added to the Oracle ILOM web interface for x86 servers and some SPARC servers.

For detailed description of the power capping properties, see [TABLE: Advanced Power Capping Policy Property Descriptions on page 82](#).

TABLE: Advanced Power Capping Policy Property Descriptions

Power Limit 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. <p>- -System -Default – Platform selected optimum grace period.</p> <p><i>or</i></p> <p>- -Custom – User-specified grace period.</p> <ul style="list-style-type: none">• 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 Oracle 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, Oracle ILOM will display a -Status -Error -Message to notify you that Oracle 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, Oracle ILOM takes the following actions:<ul style="list-style-type: none">* Display a -Status -Error -Message.* Hard-power-off the server. <p>Note - The default option for Violation Actions is -None .</p>

Note – The Advanced Power Capping Policy settings replaced the Time Limit properties originally available from the Power Management -> Budget tab in Oracle ILOM 3.0.6.

FIGURE: Advanced Power Policy Appear on Limit Tab as of Oracle ILOM 3.0.8

Power Limit

View and configure the Power Limit from this page.

Power Limiting: Enabled

Target Limit: watts percent

The value can be in watts or a percent between *Installed Hardware Minimum Power* (21 watts) and *Allocated Power* (225 watts).

Advanced Settings

Policy: Soft - Only cap if *Actual Power* exceeds *Target Limit*.
Cap power within: seconds

Hard - Fixed cap keeps *Peak Permitted* power under *Target Limit*.

Violation Actions:

System action if *Target Limit* has been exceeded.

For more information about configuring power limit properties using the Oracle ILOM web interface, see the section about Configure Server Power Limit Properties in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Power Usage Statistics and History Metrics for Server SP and CMM

As of Oracle ILOM 3.0.3, a rolling average of power consumption in 15, 30, and 60 second intervals is available for the server SP and CMM. Specifically, these rolling averages displayed by the Oracle ILOM CLI or web interface are obtained by leveraging Oracle ILOM’s sensor history capability.

Note – The power consumption history information presented in Oracle ILOM is retrieved at a rate determined by the individual platform server or CMM, which could range from 1 to 8 seconds, and typically could average between 3 to 5 seconds.

For more details about viewing the power usage and history information for a hardware device in Oracle ILOM, see the following topics:

- “Web Interface Power Usage Statistics and History Metrics” on page 84
- “CLI Power Consumption History Metrics” on page 88

Web Interface Power Usage Statistics and History Metrics

The Power Consumption History metrics for the server SP and CMM are available from the Oracle ILOM CLI and web interface.

- [“Power Usage Statistics and History as of Oracle ILOM 3.0.3”](#) on page 84
- [“Power Usage Statistics and History Web Enhancements as of Oracle ILOM 3.0.4”](#) on page 86
- [“Power Usage Statistics and Power History Web Enhancements as of Oracle ILOM 3.0.14”](#) on page 87
- [“Updated Server SP Power Allocation Web Procedure”](#) on page 96

Power Usage Statistics and History as of Oracle ILOM 3.0.3

As of Oracle ILOM 3.0.3, you can access power metrics for system Power Usage Averages and History in the Oracle ILOM web interface from the System Monitoring -> Power Management page (click History link).

FIGURE: Web Power Usage and History Metrics for CMM as of Oracle ILOM 3.0.3

Power History

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

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

Power History - Data Set Sample of Power Consumed

You can obtain a sample data set of the power consumed by the system for a specific duration by clicking the Sample Set link on the History page.

EXAMPLE: Data Set Sample of Power Consumed by System

The screenshot displays the Oracle ILOM 3.0.4 interface. At the top, there are three main tabs: "System Information", "System Monitoring", and "Power Management". Under "Power Management", there are sub-tabs: "Consumption", "Allocation", "Statistics", and "History". The "History" tab is selected, showing a "Power History" section with a sub-tab "1 Minute Average, 1 Hour History". The main content area shows a table of power consumption data.

View the data history for sample set.

Time Stamp	Power Consumed (Watts)
Sep 25 12:22:33	175
Sep 25 12:21:33	175
Sep 25 12:20:34	175
Sep 25 12:19:34	175
Sep 25 12:18:34	175
Sep 25 12:17:33	175
Sep 25 12:16:33	175
Sep 25 12:15:33	175
Sep 25 12:14:33	175
Sep 25 12:13:33	175
Sep 25 12:12:34	175
Sep 25 12:11:34	175

Power History

View the power history data from this page.

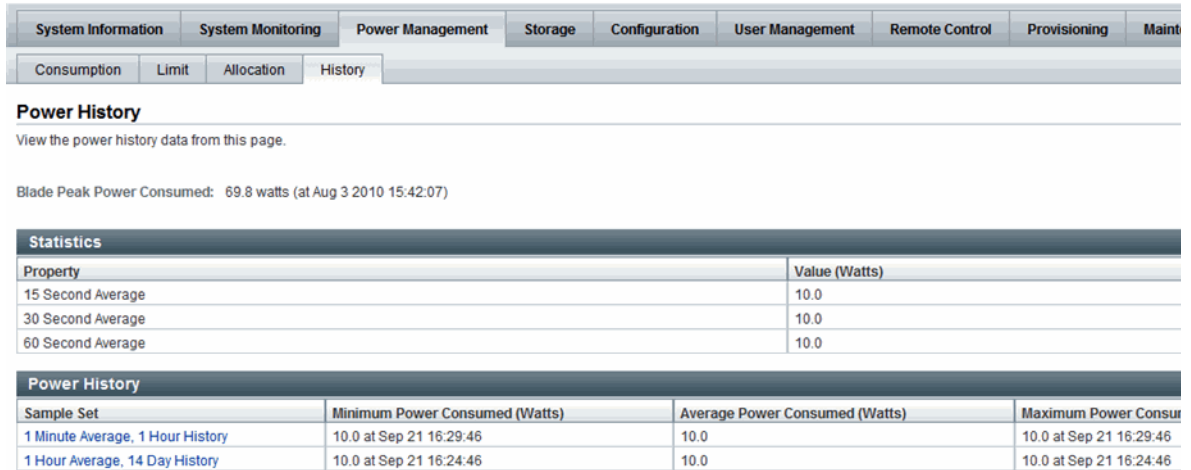
System Peak Power Consumed: 332 watts (at Jul 27 2010 15:54:47)

Sample Set	Minimum Power Consumed
1 Minute Average, 1 Hour History	175 at Sep 25 12:20:33
1 Hour Average, 14 Day History	173 at Sep 17 15:53:33

Power Usage Statistics and History Web Enhancements as of Oracle ILOM 3.0.4

As of Oracle ILOM 3.0.4, the metrics for the power usage statistics and history was removed from the Power Management page (shown in [FIGURE: Web Power Usage and History Metrics for CMM as of Oracle ILOM 3.0.3 on page 85](#)) to a separate Power Management --> History tab (shown in [FIGURE: Web Power Usage and History Metrics for CMM as of Oracle ILOM 3.0.3 on page 85](#)).

FIGURE: Web Power Statistics and Power History for Server as of Oracle ILOM 3.0.4



Power Usage Statistics and Power History Web Enhancements as of Oracle ILOM 3.0.14

As of Oracle ILOM 3.0.14, the Statistics table appearing on the Power Management --> History tab in Oracle ILOM 3.0.4 (shown in [FIGURE: Web Power Statistics and Power History for Server as of Oracle ILOM 3.0.4 on page 87](#)) was moved to a separate Statistics tab (shown in [FIGURE: Power Statistics Tab for Server as of Oracle ILOM 3.0.14 on page 87](#) and [FIGURE: Power Statistics Tab for CMM as of Oracle ILOM 3.0.14 on page 88](#)) in the Oracle ILOM web interface.

FIGURE: Power Statistics Tab for Server as of Oracle ILOM 3.0.14

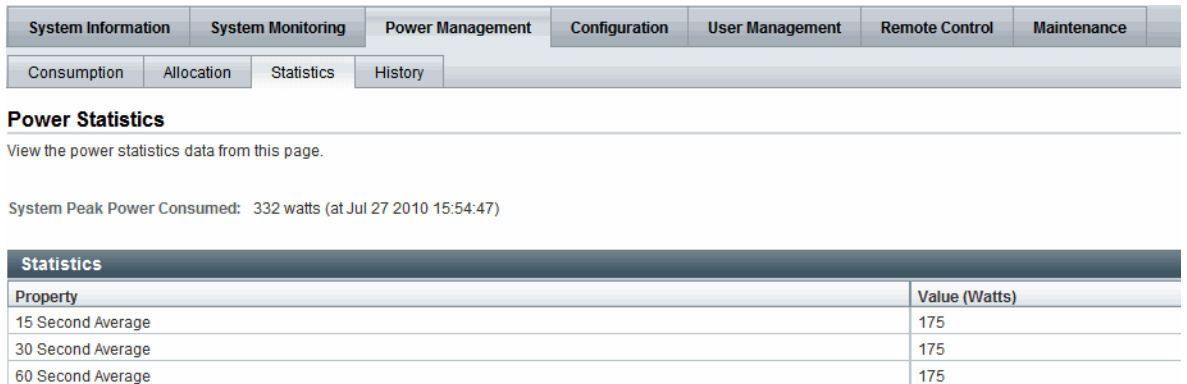


FIGURE: Power Statistics Tab for CMM as of Oracle ILOM 3.0.14

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

Power Statistics

View the power statistics data from this page.

Chassis Peak Power Consumed: 1812 watts (at May 7 1972 11:46:23)

Power Usage Averages			
Component	15 Second Average (Watts)	30 Second Average (Watts)	60 Second Average (Watts)
Chassis	No Data	922	918
Blade 0	No Data	10.0	10.0
Blade 1	No Data	72.0	72.0
Blade 2	No Data	No Data	No Data
Blade 3	No Data	No Data	No Data
Blade 4	No Data	No Data	No Data
Blade 5	No Data	74.1	73.3
Blade 6	No Data	No Data	No Data
Blade 7	No Data	76.6	75.8
Blade 8	No Data	0.00	0.00
Blade 9	No Data	10.0	10.0

FIGURE: Power History Tab for Server as of Oracle ILOM 3.0.14

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

Power History

View the power history data from this page.

System Peak Power Consumed: 332 watts (at Jul 27 2010 15:54:47)

Power History			
Sample Set	Minimum Power Consumed (Watts)	Average Power Consumed (Watts)	Maximum Power Consumed (Watts)
1 Minute Average, 1 Hour History	175 at Sep 25 12:20:33	193	252 at Sep 25 11:45:33
1 Hour Average, 14 Day History	173 at Sep 17 15:53:33	191	231 at Sep 24 09:00:00

CLI Power Consumption History Metrics

TABLE: CLI Power Consumption History Properties as of Oracle ILOM 3.0.3 on page 89 identifies the power consumption history properties available from the Oracle ILOM CLI as of Oracle ILOM 3.0.3.

TABLE: CLI Power Consumption History Properties as of Oracle ILOM 3.0.3

Power Consumption History Property	Use the <code>show</code> command to view the power consumption history value, for example:
Rolling Power Usage Averages	<ul style="list-style-type: none">• For server SPs: <code>show /SYS/VPS/history</code>• For CMMs: <code>show /CH/VPS/history</code>
Average Power Consumption	<ul style="list-style-type: none">• For server SPs: <code>show /SYS/VPS/history/0</code>• For CMMs: <code>show /CH/VPS/history/0</code>
Sample set details for time stamp and power consumed in watts	<ul style="list-style-type: none">• For server SPs: <code>show /SYS/VPS/history/0/list</code>• For CMMs: <code>show /CH/VPS/history/0/list</code>

Power Consumption Threshold Notifications as of Oracle ILOM 3.0.4

As of Oracle ILOM 3.0.4, two new Notification Threshold settings are available in the CLI and web interface (as shown in [FIGURE: Power Consumption Page as of Oracle ILOM 3.0.4 on page 76](#)). These Notification Threshold settings enable you to generate up to two power consumption notifications when the specified power consumption value (in watts) exceeds the threshold. Each time the power consumption value exceeds the specified threshold (in watts) an Oracle ILOM event is generated and logged in the Oracle ILOM event log.

The power consumption notification generated by Oracle ILOM is dependent on the whether email alerts have been configured or if SNMP traps have been enabled. For more information, about email alerts and SNMP traps, see [“System Monitoring and Alert Management” on page 39](#).

For more information about configuring the power consumption notification thresholds, see the section about View and Configure Notification Thresholds in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide.*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

Component Allocation Distribution as of Oracle ILOM 3.0.6 for Server SP and CMM

The Component Allocation Power Distribution feature in Oracle ILOM enables you to monitor, in real-time, the amount of power that is allocated to server components and, if applicable, CMM components.

Topics described in this section:

- [“Monitoring Server Power Allocated Components” on page 90](#)
- [“Monitoring CMM Power Allocated Components” on page 92](#)
- [“Component Power Allocation Special Considerations” on page 94](#)
- [“Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.8 \(Server SP\)” on page 95](#)
- [“Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.10 \(CMM\)” on page 96](#)
- [“Revised CLI Power Allocation Properties as of Oracle ILOM 3.0.10” on page 98](#)

Monitoring Server Power Allocated Components

[TABLE: Server Power Allocated Components on page 90](#) identifies the components that are allocated power in Oracle ILOM by your Oracle Sun server. For each component listed in [TABLE: Server Power Allocated Components on page 90](#), Oracle ILOM provides an allocated server power value in wattage that 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.

TABLE: Server Power Allocated Components

Server Power Allocated Component	Allocated Power (Watts)	Applicable to Rackmount Server	Applicable to Sun Blade Server Module
All server power-consuming components	X	X	X
CPUs	X	X	X
Memory modules, such as DIMMs	X	X	X
I/O modules, such as HDDs, PEMs, REMs*, RFEMs*	X	X	X

TABLE: Server Power Allocated Components (Continued)

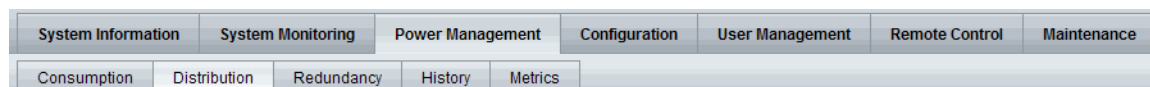
Server Power Allocated Component	Allocated Power (Watts)	Applicable to Rackmount Server	Applicable to Sun Blade Server Module
Motherboard (MB)	X	X	X
Power Supply Units (PSUs)	X	X	Does not apply [†]
Fans (FM)	X	X	Does not apply [†]

* These I/O modules apply only to Sun Blade server modules.

† These devices for server modules are allocated power by the CIMM. See [TABLE: CMM Power Allocated Components on page 93](#) for details.

You can monitor the server power allocated components from the Power Management --> Distribution page in the Oracle ILOM SP web interface or from the `SP/powermgmt/powerconf` CLI target in the Oracle ILOM SP CLI. An example of the Power Management --> Distribution page is shown in [FIGURE: Power Management --> Distribution Tab - Oracle ILOM SP 3.0.6 on page 92](#).

FIGURE: Power Management --> Distribution Tab - Oracle ILOM SP 3.0.6



Power Distribution

View and configure the power distribution from this page.

Allocated Power: 4631 watts

Power allocated to all power-consuming components in the system (includes power permanently allocated for unmanaged hot pluggable components such as I/O and fans).

Allocatable Power: 1769 watts

Power available to allocate to new blades.

Distribution Details

Each blade slot allocates a minimum of 146 watts to accommodate I/O blades.

Blade Slot Power Distribution			
<input type="button" value="Edit"/>			
	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

For more details about how to view the server or CMM power allocation, see the sections about View Server Component Power Allocation or View CMM Component Power Allocation in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Update: As of Oracle ILOM 3.0.8 the Distribution tab is replaced by the Allocation tab. For more details, see [“Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.8 \(Server SP\)”](#) on page 95 or [“Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.10 \(CMM\)”](#) on page 96.

Monitoring CMM Power Allocated Components

[TABLE: CMM Power Allocated Components](#) on page 93 identifies the components that are allocated power in Oracle ILOM by the CMM in your Sun system chassis. For each component listed in [TABLE: CMM Power Allocated Components](#) on

page 93, Oracle ILOM provides an allocated CMM power value in wattage that represents the sum of the maximum power consumed by either a single CMM component (a blade), a category of CMM components (all blades), or all CMM power-consuming components. It also provides a permitted CMM power value in wattage that represents the guaranteed maximum power the CMM component (or component category) can consume.

Note – The *Permitted Power* value in Oracle ILOM is derived from the *Power Supply Redundancy Policy* and the *Redundant Power* available (for details see, “[Power Supply Redundancy for CMM Systems as of Oracle ILOM 3.0.6](#)” on page 105). The CMM continuously monitors and tracks all the *Allocated Power* to the system, as well as the *Allocatable Power* remaining and it ensures that the sum for these numbers (allocated and allocatable) never exceeds the chassis *Permitted Power* value.

Note – Power to a Sun Blade server module is allocated by the CMM when a request for power is made by the server module. The server module requests power whenever it is powered on, and releases power back to the CMM whenever it is powered off. The CMM allocates power to the server module if the remaining allocatable power is sufficient to meet the server module’s request. The CMM also checks whether there is a limit set to the amount of power that it is permitted to a server module (which is known as the *Blade Slot Permitted Power* in the web interface or `CMM/powermgmt/powerconf/bladeslots/BLn permitted_power` in the CLI). The CMM only allocates power to the server module if the requested power is less than or equal to this property.

TABLE: CMM Power Allocated Components

CMM Power Allocated Component	Allocated Power (Watts)	Permitted Power (Watts)	Allocatable Power (Watts)
All CMM power-consuming components (aggregate value for all powered entities listed)	X	X	X
Blade slots (BL#)	X	X*	Does not apply
CMM	X	Does not apply	Does not apply
Network Express Modules (NEMs)	X	Does not apply	Does not apply
Power Supply Units (PSUs)	X	Does not apply	Does not apply
Fans (FM)	X	Does not apply	Does not apply

* The permitted power allocated to slots is user configurable.

You can monitor the power allocated CMM components from the Power Management --> Distribution page in the Oracle ILOM CMM web interface or from the CMM/powermgmt/powerconf CLI target in the Oracle ILOM CMM CLI. For instructions, see the section about View CMM Component Power Allocation in one of the following guides.

- *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

In addition to monitoring the power allocation for each CMM power allocated component, you can modify the permitted (maximum) power the CMM allocates to blade slots within the chassis. For instructions, see the section about Configure Permitted Power for Blade Slots in one of the following guides:

- *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Component Power Allocation Special Considerations

When monitoring the server or CMM power allocated components, consider the following information:

- **Power allocation for component categories.** For component categories that include multiple components, such as fans, you will be able to monitor the total sum of power consumed by all components (fans), as well as the total sum of power consumed by an individual component (fan).
- **Hot-pluggable component power allocation.** Oracle ILOM automatically displays a pre-allocated maximum power value for any known component that can be placed in a hot-plug component location either on a server or on a system chassis. For example:
 - A hot-pluggable component location on an Oracle Sun server could include storage slots for hard disk drives (HDDs). In this case, Oracle ILOM will display a maximum power value for the HDD to be placed in the storage slot.
 - A hot-pluggable component location on a system chassis (with a CMM) can include blade slots for server modules or I/O server modules. In this case, Oracle ILOM will display a maximum power value for any I/O server module that could be placed in the blade slots. However, if I/O server modules are not supported in the system chassis, then Oracle ILOM will display a maximum power value for a server module (and not an I/O server module).

For more information about which locations or components on your server or CMM chassis system are hot-pluggable, refer to the platform documentation shipped with your system.

- **Power supply power allocation.** Oracle ILOM automatically allocates power to the power supply to account for power losses between the wall outlet and the component.

- **Troubleshooting Sun Blade server module power-on issues.** If the Sun Blade server module is unable to power on, verify that the SP permitted power property value (`/SP/powermgmt permitted_power`) is not more than the CMM blade slot permitted power property value (`/CMM/powermgmt/powerconf/bladeslots/BLn permitted_power`).

Note – Oracle ILOM 3.x server modules negotiate with the CMM and honor the permitted power restriction. Pre-3.x Oracle ILOM server modules will power on as long as there is enough allocatable power. Therefore, the permitted power constraint is only honored by server modules running Oracle ILOM 3.x or subsequent release.

Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.8 (Server SP)

The Distribution tab that was previously available for the server SP in Oracle ILOM 3.0.6 (shown in [FIGURE: Power Management --> Allocation Tab - Oracle ILOM SP 3.0.8 on page 96](#)) was renamed in Oracle ILOM 3.0.8 to the Allocation tab (shown in [FIGURE: Power Management --> Allocation Tab - Oracle ILOM SP 3.0.8 on page 96](#)).

The Allocation tab, in Oracle ILOM 3.0.8, provides all the same power requirement information previously available on the Distribution tab in Oracle ILOM 3.0.6 (shown in [FIGURE: Power Management --> Distribution Tab - Oracle ILOM SP 3.0.6 on page 92](#)). However, the Allocation tab uses two tables to separate the system power requirements from the component power requirements (shown in [FIGURE: Power Management --> Allocation Tab - Oracle ILOM SP 3.0.8 on page 96](#)).

FIGURE: Power Management --> Allocation Tab - Oracle ILOM SP 3.0.8

System Information	System Monitoring	Power Management	Configuration	User Management	Remote Control	Maintenance
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 Capped
CPUs (total)	60	Yes
MB_P0	60	Yes
memory (total)	10	No
MB_P0_D8	10	No
I/O (total)	80	No
HDD0	8	No
HDD1	8	No
HDD2	8	No
HDD3	8	No
MB_REM	18	No
PEM0	15	No
PEM1	15	No
MB	75	No

Updated Server SP Power Allocation Web Procedure

For instructions for viewing the server power allocations in Oracle ILOM, see the section about View Server Power Allocation Plan in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Power Management --> Distribution Tab Renamed to Allocation Tab as of Oracle ILOM 3.0.10 (CMM)

The Distribution tab that was previously available for the CMM in Oracle ILOM 3.0.6 (shown in [FIGURE: Power Management --> Distribution Tab - Oracle ILOM SP 3.0.6 on page 92](#)) was renamed in Oracle ILOM 3.0.10 to the Allocation tab (shown in [FIGURE: Power Management -> Allocation Tab - Oracle ILOM CMM 3.0.10 on page 98](#)).

The Allocation tab, in Oracle ILOM 3.0.10, provides all the same power requirement information previously available on the CMM Power Distribution tab in Oracle ILOM 3.0.6. However, the new CMM Allocation tab in Oracle ILOM 3.0.10 provides two additional tables that identify the System Power Specifications and the Blade Power Grants (as shown in [FIGURE: Power Management -> Allocation Tab - Oracle ILOM CMM 3.0.10 on page 98](#)).

[TABLE: New or Revised Properties on CMM Allocation Tab on page 97](#) defines the property changes made on the CMM Allocation Tab as of 3.0.10.

TABLE: New or Revised Properties on CMM Allocation Tab

Updated Property Name	Details
Grantable Power (renamed property)	Allocatable Power in Oracle ILOM 3.0.6 was renamed to Grantable Power in Oracle 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 Oracle ILOM 3.0.6 was renamed to Grant Limit in Oracle 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, the procedure for Configure Grant Limit for Blade Slots in the <i>Oracle Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide</i> .
Granted Power (renamed property)	Allocated Power in Oracle ILOM 3.0.6 was renamed to Granted Power in Oracle 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.

FIGURE: Power Management -> Allocation Tab - Oracle ILOM CMM 3.0.10

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

Revised CLI Power Allocation Properties as of Oracle ILOM 3.0.10

A summary of the CLI changes that were made in Oracle ILOM 3.0.10 to the CMM power configuration is provided in [TABLE: New Power Management CLI Properties in Oracle ILOM 3.0.10](#) on page 99.

TABLE: New Power Management CLI Properties in Oracle ILOM 3.0.10

Renamed CLI Properties	Details
allocated_power renamed to granted_power for blade slots	The following CLI allocated_power property for all blade slots in Oracle ILOM 3.0.6: <code>/CMM/powermgmt/powerconf/bladeslot allocated_power</code> changed in Oracle ILOM 3.0.10 to granted_power: <code>/CMM/powermgmt/powerconf/bladeslot granted_power</code>
allocated_power renamed granted_power for blades	The following CLI allocated_power property for blades in Oracle ILOM 3.0.6: <code>/CMM/powermgmt/powerconf/bladeslot/BLn allocated_power -> granted_power</code> changed in Oracle ILOM 3.0.10 to granted_power: <code>/CMM/powermgmt/powerconf/bladeslot/BLn granted_power</code>
permitted_power renamed grant_limit for blades	The following CLI permitted_power property for blades in Oracle ILOM 3.0.6: <code>/CMM/powermgmt/powerconf/bladeslot/BLn permitted_power</code> changed in Oracle ILOM 3.0.10 to grant_limit: <code>/CMM/powermgmt/powerconf/bladeslot/BLn grant_limit</code>

For instructions for using these latest CLI properties to view granted power or grant limit per blade, see the procedures about View Granted Power or Grant Limit in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Power Budget as of Oracle ILOM 3.0.6 for Server SPs

Note – The Power Budget properties described in this section are replaced in the web interface with the Limit tab properties as of Oracle ILOM 3.08. For updated details, see.

Some Oracle server platforms support a power budget. A power budget sets a limit on the system's power consumption. The system applies power capping when power consumption exceeds the power limit and guarantees that the maximum power consumption will not exceed the system's Permitted Power.

You can configure a power budget and then, at a later time, enable or disable the configuration properties that are set. After a power budget is enabled, the Oracle ILOM SP monitors the power consumption and applies power capping when needed. Power capping is achieved by limiting the maximum frequency at which the

CPUs run. The Oracle ILOM SP coordinates this process with the operating system (OS) to ensure that the OS can continue applying its own power management policies within the set limit.

Power budget settings in Oracle ILOM are saved across all SP reboots and host power-off and power-on states. During an SP reboot, the applied power capping budget that is in effect will remain. After the SP completes the reboot process, power capping is then automatically adjusted, as needed, by the system.

Oracle ILOM's ability to achieve a power budget depends on the workload running on the system. For example, if the workload is causing the system to operate near the maximum power consumption, Oracle ILOM will be unable to achieve a budget that is close to the minimum power consumption. If Oracle ILOM is unable to achieve the set `Power Limit`, it will automatically generate a violation notification.

For information about configuring Power Budget properties in the Oracle ILOM, see the section about Configure Server Power Budget Properties in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Power Budget topics described in this section include:

- [“Why Use a Power Budget?” on page 100](#)
- [“Server Power Budget Properties as Oracle ILOM 3.0.6” on page 101](#)
- [“Advanced Server Power Budget Features as of Oracle ILOM 3.0.6” on page 101](#)
- [“Power Management --> Budget Tab Renamed to Limit Tab as of Oracle ILOM 3.0.8” on page 103](#)

Why Use a Power Budget?

The Power Budget feature in Oracle ILOM helps you to better plan and manage the power required for your data center. Typically the power allocated to a server is based on the nameplate power, as provided by the `/SP/powermgmt allocated_power` property.

The most effective way to use the Power Budget feature in Oracle ILOM is to:

1. Determine the workload that will operate on the Oracle server.
2. Set the `Power Limit` property in Oracle ILOM that is near (for example, at or slightly above) to the workload's normal operating power consumption.
3. Use the `Power Limit` property value to help plan the amount of power that will need to be allocated in your data center for this system.

Server Power Budget Properties as Oracle ILOM 3.0.6

[TABLE: Server Power Budget Properties as of Oracle ILOM 3.0.6 on page 101](#) identifies the server power budget properties that you can view or configure from the CLI or web interface in Oracle ILOM.

TABLE: Server Power Budget Properties as of Oracle ILOM 3.0.6

Power Budget Property	Description
Activation State	Enable this property to enable the power budget configuration.
Status	<p>The Status reports one of the following current power budget states:</p> <ul style="list-style-type: none">• OK – The OK status appears when the system is able to achieve the power limit, or when the power budget is not enabled.• Violation – The Violation status occurs when the system is not able to reduce power to the power limit. <p>If the power consumption falls below the <code>Power Limit</code>, the violation is cleared and the status returns to <code>ok</code>.</p> <p>The budget status is also reported through a system sensor: <code>/SYS/PWRBS</code>. This is a discreet sensor which is set to 1 (deasserted) when the budget is <code>ok</code>, and to 2 (asserted) when the budget has been violated.</p>
Power Limit	<p>Set a <code>Power Limit</code> in watts or as a percentage of the range between minimum and maximum system power.</p> <p>Note - The minimum system power is viewable in the CLI under the target <code>/SP/powermgmt/budget_min_powerlimit</code>. The maximum system power is viewable from the <code>Allocated Power</code> property in the web interface or from the CLI under the target <code>/SP/powermgmt/allocated_power</code>.</p>

Advanced Server Power Budget Features as of Oracle ILOM 3.0.6

The advanced server power budget features in Oracle ILOM include properties for `Time Limit` and `Violation Actions`. These property settings (see [TABLE: Advanced Server Power Budget Properties as of Oracle ILOM 3.0.6 on page 102](#)) enable you to control the aggressiveness of power capping, and to configure a system action in response to a violated budget.

The server power budget is designed to ensure that power capping is not applied until the `Power Limit` is exceeded. The `Time Limit` property specifies the grace period for capping power to within the `Power Limit`, if exceeded. The system provides a default grace period that is set to achieve responsiveness at the least cost to the system performance. When the default grace period is enabled for the `Time Limit` property, anomalous spikes are ignored and power capping is applied only when power consumption remains above the `Power Limit`. If you specify a different grace period than the default grace period provided, the user-modified grace period could cause Oracle ILOM to increase or decrease the power cap severity in response to exceeding the `Power Limit`.

Server modules are allocated power by the chassis CMM, and must guarantee to not exceed this allocated amount. It might be necessary to reduce the server module's guaranteed maximum power to allow the server module to power on, or there might be some other administrative reason for requiring that the server power never exceeds a watts value. Setting the budget grace period to `None` instructs Oracle ILOM to permanently apply power capping to ensure that the `Power Limit` is never exceeded, at the cost of limited performance. If Oracle ILOM can guarantee the `Power Limit` with a grace period of `None`, it reduces the value of the `Permitted Power` property to reflect the new guaranteed maximum power. If the power limit or grace period is later increased, the `Permitted Power` value on a rackmount server is increased. However, the `Permitted Power` value for a Sun Blade server module will only increase if the chassis CMM is able to provide the server module with additional power.

[TABLE: Advanced Server Power Budget Properties as of Oracle ILOM 3.0.6 on page 102](#) identifies the advanced server power budget property settings that you can view or configure from the Oracle ILOM CLI or web interface.

TABLE: Advanced Server Power Budget Properties as of Oracle ILOM 3.0.6

Power Budget Property	Description
Time Limit	Specify one of the following grace periods for capping the power usage to the limit: <ul style="list-style-type: none"> • Default – Platform selected optimum grace period. • None – No grace period. Power capping is permanently applied. • Custom – User-specified grace period.
Violation Actions	The actions that the system will take if the power limit cannot be achieved within the grace period. This option can be set to <code>-None</code> or <code>-Hard Power Off</code> . This setting, by default, is set to <code>None</code> .

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

An example of the web interface Power Management --> Budget properties is shown in [FIGURE: SP - Power Management Budget Tab - Oracle ILOM 3.0.6](#) on page 103.

FIGURE: SP - Power Management Budget Tab - Oracle ILOM 3.0.6

The screenshot shows the Oracle ILOM web interface with the following structure:

- Navigation tabs: System Information, System Monitoring, Power Management (selected), Configuration, User Management, Remote Control, Maintenance.
- Sub-tabs under Power Management: Consumption, Distribution, Budget (selected), History.
- Section: **Power Budget Management**
- Text: View and configure the power budget from this page.
- Activation State: Enabled
- Status: OK
- Power Limit: watts percent
Upper limit of system power usage. Power capping is applied if the power limit is exceeded. The value can be in watts or a percent between minimum power limit (67 watts) and Allocated Power (265 watts).
- Time Limit: seconds
Grace period for capping power to the powerlimit if exceeded. 'None' forces permanent capping.
- Violation Actions:

For instructions about how to view or configure the server and advanced server power budget properties in Oracle ILOM, see the section about Configure Server Power Budget Properties in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Power Management --> Budget Tab Renamed to Limit Tab as of Oracle ILOM 3.0.8

The Budget tab that was previously available for server SPs in Oracle ILOM 3.0.6 was renamed in Oracle ILOM 3.0.8 to the Limit tab (shown in [FIGURE: Power Management --> Limit Tab - Oracle ILOM SP 3.0.8](#) on page 105).

The Limit tab in Oracle ILOM 3.0.8 provides all the same SP power capping information that was previously available on the Budget tab. However, some of the previous power capping properties have been renamed on the Power Management

--> Limit tab in Oracle ILOM 3.0.8. For more details about the property changes made to the Limit tab, see [TABLE: Limit Tab Server SP Setting Changes in Oracle ILOM 3.0.8 on page 104](#).

TABLE: Limit Tab Server SP Setting Changes in Oracle ILOM 3.0.8

Limit Tab Property Changes	Details
-Power -Limiting (renamed property)	<p>The -Activation -State property on the Budget tab in Oracle ILOM 3.0.6 (shown in FIGURE: SP - Power Management Budget Tab - Oracle ILOM 3.0.6 on page 103) was renamed to -Power -Limiting on the Power Management --> Limit tab in Oracle ILOM 3.0.8.</p> <p>The -Powering -Limiting -[] -enable property (shown in FIGURE: Power Management --> Limit Tab - Oracle ILOM SP 3.0.8 on page 105) when selected enables the power limit configuration.</p>
-Status -Error -Message (replaces -Status property)	<p>The -Status read-only property previously available on the Budget tab in Oracle ILOM 3.0.6 (shown in FIGURE: SP - Power Management Budget Tab - Oracle ILOM 3.0.6 on page 103) was replaced by a new Status Error Message on the Power Management --> Limit tab or Consumption tab in Oracle ILOM 3.0.8 (shown in FIGURE: Sample Power Management Metrics Page on page 107).</p> <p>The new Status Error Message only appears on your system when Oracle ILOM fails to achieve the power limit that was configured.</p>
-Target -Limit (renamed property)	<p>The -Power -Limit property on the Budget tab in Oracle ILOM 3.0.6 (shown in FIGURE: Power Management --> Limit Tab - Oracle ILOM SP 3.0.8 on page 105) was renamed to -Target -Limit on the Power Management --> Limit tab in Oracle ILOM 3.0.8.</p> <p>The -Target -Limit property (shown in FIGURE: Power Management --> Limit Tab - Oracle ILOM SP 3.0.8 on page 105) enables you to specify the a target limit value in watts or as a percentage. This value must be a range between the minimum and maximum system power.</p>
-Policy (renamed advanced property)	<p>The -Time -Limit property on the Budget tab in Oracle ILOM 3.0.6 (shown in FIGURE: SP - Power Management Budget Tab - Oracle ILOM 3.0.6 on page 103) was renamed to -Policy on the Power Management --> Limit tab in Oracle ILOM 3.0.8.</p> <p>The -Policy property (shown in FIGURE: Power Management --> Limit Tab - Oracle ILOM SP 3.0.8 on page 105) enables you to specify the type of power capping 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. <p>- -System -Default – Platform selected optimum grace period.</p> <p><i>or</i></p> <p>- -Custom – User-specified grace period.</p> <ul style="list-style-type: none"> • Hard - Fixed cap keeps Peak Permitted power under Target Limit – If you enabled this option, power capping is permanently applied without a grace period.

An example of the new Power Management --> Limit tab properties that are available for server SPs as of Oracle ILOM version 3.0.8 is shown in [FIGURE: Power Management --> Limit Tab - Oracle ILOM SP 3.0.8](#) on page 105.

FIGURE: Power Management --> Limit Tab - Oracle ILOM SP 3.0.8

The screenshot displays the Oracle ILOM web interface for configuring Power Limit properties. The top navigation bar includes tabs for System Information, System Monitoring, Power Management (selected), Configuration, User Management, Remote Control, and Maintenance. Under the Power Management tab, there are sub-tabs for Consumption, Limit (selected), Allocation, and History. The main content area is titled "Power Limit" and contains the following configuration options:

- Power Limiting:** A checkbox labeled "Enabled" is checked.
- Target Limit:** A text input field contains the value "189". To its right are radio buttons for "watts" (selected) and "percent". Below this is a note: "The value can be in watts or a percent between *Installed Hardware Minimum Power* (21 watts) and *Allocated Power* (225 watts)."
- Advanced Settings:**
 - Policy:** Radio buttons for "Soft - Only cap if *Actual Power* exceeds *Target Limit*." (selected) and "Hard - Fixed cap keeps *Peak Permitted* power under *Target Limit*." are present. Below the "Soft" option is a "Cap power within:" label, a dropdown menu set to "System Default", and a text input field for "seconds".
 - Violation Actions:** A dropdown menu is set to "None". Below it is a note: "System action if *Target Limit* has been exceeded."

A "Save" button is located at the bottom left of the configuration area.

Updated Power Limit Configuration Procedure

For information about configuring Power Limit properties in Oracle ILOM, see the section about Configure Server Power Limit Properties in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Power Supply Redundancy for CMM Systems as of Oracle ILOM 3.0.6

From the Oracle ILOM CMM CLI or web interface you can view and configure the following power supply redundancy options:

- **Power Supply Redundancy Policy** – This policy controls the number of power supplies that are currently allocating power in addition to the number of power supplies that are reserved to handle power supply failures. Values for this redundancy policy property can be set to:
 - **None** – Reserves no power supplies.

- **n+n** – Reserves half of the power supplies to handle power supply failures.
- **Redundant Power** – This value is provided by the system. It represents the available power that is not allocated.

To view or configure the CMM power supply redundancy options in the Oracle ILOM CLI or web interface, see the section about View or Configure CMM Power Supply Redundancy Properties in one of the following guides:

- *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Platform-Specific CMM Power Metrics as of Oracle ILOM 3.0.6

Note – As of Oracle ILOM 3.0.10, the CMM Power Metrics tab was removed from the Oracle ILOM CLI and web interface.

As of Oracle ILOM version 3.0.6, advanced power metrics are available in some Oracle systems from the Oracle ILOM CMM CLI or web interface. These metrics represent the maximum allocated power value for each blade slot. For empty slots or slots with I/O server modules, the value presented by Oracle ILOM represents the maximum power that an I/O server module could consume.

To determine whether your CMM system supports this Oracle ILOM 3.0.6 feature, refer to the platform Oracle ILOM Supplement for your server or CMM.

For Oracle systems supporting the CMM advanced power metrics, you can view the power metrics in the Power Management --> Metrics page of the Oracle ILOM web interface ([FIGURE: Sample Power Management Metrics Page on page 107](#)) or from the Oracle ILOM CLI under the target `/CMM/powermgmt/advanced/BLn`.

FIGURE: Sample Power Management Metrics Page

The screenshot shows a web interface for power management. At the top, there is a navigation menu with tabs for System Information, System Monitoring, Power Management, Configuration, User Management, Remote Control, and Maintenance. Below this, a sub-menu is visible with tabs for Consumption, Distribution, Redundancy, History, and Metrics. The main content area is titled "Power Metrics" and contains a sub-section "Advanced Power Metrics" which displays a table of power metrics.

Power Metrics

View the power management metrics from this page.

Advanced Power Metrics		
Name	Unit	Value
BL0 Max Power	Watts	728
BL1 Max Power	Watts	502
BL2 Max Power	Watts	728
BL3 Max Power	Watts	0
BL4 Max Power	Watts	0
BL5 Max Power	Watts	455
BL6 Max Power	Watts	0
BL7 Max Power	Watts	0
BL8 Max Power	Watts	0
BL9 Max Power	Watts	0

Remote Host Management Operations

Description	Links
Learn about controlling the power state of a remote server.	<ul style="list-style-type: none">• “Remote Power Control” on page 110
Learn how to control the host boot device on an x86 system SP.	<ul style="list-style-type: none">• “Host Control - Boot Device on x86 Systems” on page 110
Learn about Logical Domain (LDom) configurations on SPARC servers.	<ul style="list-style-type: none">• “Oracle ILOM Operations for LDom Configurations on SPARC Servers” on page 111
Learn about Oracle ILOM CLI and web remote redirection consoles.	<ul style="list-style-type: none">• “Remote Redirection Console Options” on page 111

Related Information

- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage remote host power states
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage SPARC LDOM states
- *Oracle ILOM 3.0 Daily Management Web Procedures*, manage remote host power states
- *Oracle ILOM 3.0 Daily Management Web Procedures*, manage SPARC LDOM states
- *Oracle ILOM 3.0 Remote Redirection Consoles*, Oracle ILOM Remote Console
- *Oracle ILOM 3.0 Remote Redirection Consoles*, Oracle ILOM Storage Redirection CLI

Remote Power Control

The remote power states in Oracle ILOM are available for all Oracle Sun servers from the Oracle ILOM CLI or web interface. These options enable you to control the power state of a remote host server or chassis.

For information about remotely managing the power states on a managed device, see the section about Managing Host Remote Power States in one of the following guides:

- *Oracle ILOM 3.0 Daily Management CLI Procedures*
- *Oracle ILOM 3.0 Daily Management Web Procedures*

Host Control - Boot Device on x86 Systems

As of Oracle ILOM 3.0.3, you can use the Host Control features in the CLI and web interface to select the host boot device settings that will override the boot device order in the BIOS. This ability gives the CLI and web interface parity with the existing IPMI interface.

The primary purpose of the boot device override feature is to enable the administrator to perform a one-time manual override of the server's BIOS boot order settings. This enables the administrator to quickly configure a machine or group of machines to boot from another device, such as the PXE boot environment.

The Host Control boot device settings are available in Oracle ILOM for Oracle Sun x86 systems SPs. This feature is not supported on the CMM. For Host Control settings in Oracle ILOM specific to SPARC system server SPs, consult the Oracle ILOM Supplement guide or platform Administration guide provided for that system.

For procedures on how to use the Host Control boot settings in Oracle ILOM on an x86 system SP, see the Remote Management Option procedures in the following Oracle ILOM guides:

- *Oracle ILOM 3.0 Daily Management CLI Procedures*
- *Oracle ILOM 3.0 Daily Management Web Procedures*

Oracle ILOM Operations for LDom Configurations on SPARC Servers

You can use Oracle ILOM to perform the following tasks on SPARC servers that have stored Logical Domain (LDom) configurations.

Task	Supported Oracle ILOM Point Release
View Oracle ILOM CLI targets and properties for stored LDom configurations from a host SPARC T3 Series server.	<ul style="list-style-type: none">• 3.0.12 (CLI only)• 3.0.14 (CLI and web interface)
Specify which stored LDom configuration is used on the host SPARC server when the server is powered-on.	<ul style="list-style-type: none">• 2.0.0 (CLI and web interface)
Enable (default) or disable the control domain boot property values from the host SPARC server.	<ul style="list-style-type: none">• 2.0.0 (CLI and web interface)

For more information and procedures on how to view and configure LDom configurations on SPARC servers, see the following Oracle ILOM guides:

- *Oracle ILOM 3.0 Daily Management CLI Procedures Guide*, manage LDOM states
- *Oracle ILOM 3.0 Daily Management Web Procedures*, manage LDOM states

Remote Redirection Console Options

Oracle ILOM 3.0 supports the following remote redirection console options:

- Oracle ILOM Remote Console – Web-based remote KVMs console.
- Oracle ILOM Remote Redirection Console – CLI-based remote storage redirection console

For detailed information about these remote redirection console options, see the *Oracle ILOM 3.0 Remote Redirection Console – CLI and Web Guide*.

Oracle ILOM Host Maintenance and Diagnostics Options

Description	Links
List of host maintenance operations available in Oracle ILOM.	<ul style="list-style-type: none">• “Host Maintenance Operations” on page 113
List of host diagnostic options available in Oracle ILOM.	<ul style="list-style-type: none">• “Host Diagnostic Options” on page 114

Related Information

- *Oracle ILOM 3.0 Maintenance and Diagnostics*, launch embedded version of Oracle ILOM Installation Assistant
- *Oracle ILOM 3.0 Maintenance and Diagnostics*, back up and restore Oracle ILOM configuration
- *Oracle ILOM 3.0 Maintenance and Diagnostics*, update Oracle ILOM firmware
- *Oracle ILOM 3.0 Maintenance and Diagnostics*, x86 server diagnostics
- *Oracle ILOM 3.0 Maintenance and Diagnostics*, SPARC server diagnostics
- *Oracle ILOM 3.0 Maintenance and Diagnostics*, Oracle Service diagnostics

Host Maintenance Operations

Oracle ILOM 3.0 supports the following maintenance operations:

- Embedded Oracle Hardware Installation
- Oracle ILOM firmware updates
- Back up, restore, and reset Oracle ILOM configurations

For detailed information about these host maintenance operations, see the *Oracle ILOM 3.0 Maintenance and Diagnostics CLI and Web Guide*.

Host Diagnostic Options

Oracle ILOM 3.0 supports the following host diagnostic options:

- x86 server host diagnostic tools
- SPARC server host diagnostic tools
- Oracle Service related diagnostic tools

For detailed information about using these host diagnostic options, refer to the *Oracle ILOM 3.0 Oracle ILOM 3.0 Maintenance and Diagnostics CLI and Web Guide*.

Example Setup of Dynamic DNS

This appendix describes how to configure the Dynamic Domain Name Service (DDNS) on a typical customer's infrastructure. The instructions and example configuration provided here do not affect Oracle ILOM or the service processor (SP).

The following topics are covered in this appendix:

- [“Dynamic DNS Overview” on page 115](#)
- [“Example Dynamic DNS Configuration” on page 117](#)

Dynamic DNS Overview

Once DDNS is configured, new Oracle ILOM systems will be automatically assigned a host name and an IP address at install time. Thus, once you have configured DDNS, clients can use either host names or IP addresses to access any Oracle ILOM SPs that have been added to the network.

By default, Oracle ILOM systems are shipped with Dynamic Host Configuration Protocol (DHCP) enabled so that you can use DHCP to configure the SP's network interface. With DDNS, you can further leverage DHCP to automatically make the DNS server aware of the host names of Oracle ILOM systems that have been added to the network and configured using DHCP.

Note – Domain Name Service (DNS) support, which was added to Oracle ILOM in the 3.0 release, allows hosts such as NTP servers, logging servers, and firmware upgrade servers, to be referred to within the Oracle ILOM command-line interface (CLI) and other user interfaces by host name or IP address. DDNS support, as described in this appendix, allows SPs to be referred to by their host names without being manually configured.

Oracle ILOM systems are assigned well-known host names consisting of a prefix followed by a hyphen and the Oracle ILOM SP product serial number. For rackmounted systems and server modules, the host name will consist of the prefix SUNSP and the product serial number. For a server chassis with multiple chassis

monitoring modules (CMMs), the host name for each CMM will consist of the prefix SUNCMMn and the product serial number, where n is 0 or 1. For example, given a product serial number of 0641AMA007, the host name for a rackmounted system or a server module would be SUNSP-0641AMA007. For a server chassis with two CMMs, the host names for the CMMs would be SUNCMM0-0641AMA007 and SUNCMM1-0641AMA007.

Once DDNS has been configured, SP/DHCP/DNS transactions are automatically executed to add new host names and associated IP addresses to the DNS database. Each transaction comprises the following steps:

1. Oracle ILOM creates the SP host name using the appropriate prefix and the product serial number and the Oracle ILOM SP sends the host name to the DHCP server as part of the DHCP request.
2. When the DHCP server receives the request, it assigns an IP address to the Oracle ILOM SP from an available pool of addresses.
3. The DHCP server then sends an update to the DNS server to notify it of the newly configured Oracle ILOM SP's host name and IP address.
4. The DNS server updates its database with the new information, thus completing the SP/DHCP/DNS transaction.

Once an SP/DHCP/DNS transaction is completed for a given host name, clients can make a DNS request using that host name and DNS will return the assigned IP address.

To determine the host name of a particular Oracle ILOM SP, simply check the product serial number on the outside of the SP itself and combine the product serial number with the appropriate prefix as described above. You can also determine host names by checking the server logs for DNS zone update messages.

Note – You can use the CLI to change the SP host name to something other than the default. However, if you change the host name to a non-default name, clients must use that host name to refer to the SP using DNS.

The DNS information is updated when a DHCP lease renewal causes an IP address change, and the DNS information is deleted when the DHCP lease is released.

Note – For all Oracle ILOM SPs that have been assigned host names prior to DDNS support or that may have been configured using DDNS and MAC address-based host names, the previously configured host names will remain in effect.

Example Dynamic DNS Configuration

This section describes how to set up an example DDNS configuration. You can use the procedures and sample files provided here, with site-specific modifications, to set up your own DDNS configuration.

Note – How you set up DDNS depends on the infrastructure in use at your site. Solaris, Linux, and Windows operating systems all support server solutions that offer DDNS functionality. This example configuration uses Debian r4.0 as the server operating system environment.

The following topics are covered in this section:

- [“Assumptions” on page 117](#)
- [“Configure and Start the DHCP and DNS Servers” on page 117](#)
- [“References” on page 119](#)

Assumptions

This example configuration is based on the following assumptions:

- There is a single server that handles both DNS and DHCP for the network the SP resides on.
- The SP network address is 192.168.1.0.
- The DHCP/DNS server address is 192.168.1.2
- The IP addresses from 192.168.1.100 to 192.168.1.199 are used as a pool to provide addresses to the SP and other clients.
- The domain name is `example.com`.
- There is no existing DNS or DHCP configuration in place. If there is, use the following files as a guideline to update the existing configuration.

▼ Configure and Start the DHCP and DNS Servers

To configure the servers, follow these steps:

1. **Install the `bind9` and `dhcp3-server` packages from the Debian distribution.** Installing the `dnsutils` package provides access to `dig`, `nslookup` and other useful tools as well.

2. Using `dnssec-keygen`, generate a key to be shared between the DHCP and DNS servers to control access to the DNS data.
3. Create a DNS configuration file named `/etc/bind/named.conf` that contains the following:

```
options {
    directory "/var/cache/bind";
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/etc/bind/db.root";
};
// be authoritative for the localhost forward and reverse zones,
// and for broadcast zones as per RFC 1912
zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
// additions to named.conf to support DDNS updates from dhcp server
key server.example.com {
    algorithm HMAC-MD5;
    secret "your-key-from-step-2-here"
};
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
    allow-update { key server.example.com; };
};
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.example.rev";
    allow-update { key server.example.com; };
};
```

4. Add empty zone files for the local network.

Empty zone files should be named `/etc/bind/db.example.com` and `/etc/bind/db.example.rev`.

Copying the distribution supplied `db.empty` files is sufficient; they will be updated automatically by the DNS server.

5. Create a `/etc/dhcp3/dhcpd.conf` file that contains the following:

```
ddns-update-style interim;
ddns-updates          on;
server-identifier     server;
ddns-domainname      "example.com.";
ignore client-updates;
key server.example.com {
    algorithm hmac-md5;
    secret your-key-from-step-2-here;
}
zone example.com. {
    primary 127.0.0.1;
    key server.example.com;
}
zone 1.168.192.in-addr.arpa. {
    primary 127.0.0.1;
    key server.example.com;
}
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.199;
    option domain-name-servers 192.168.1.2;
}
```

6. After completing steps 1 through 5 above, run the `/etc/init.d` script to start the DNS and DHCP servers.

Once the servers are running, any new Oracle ILOM SPs configured for DHCP will be automatically accessible using their host name when they are powered on. Use `log` files, `dig`, `nslookup`, and other utilities for debugging, if necessary.

References

For more information on the Linux DHCP and DNS servers used in this example, see the Internet Systems Consortium web site at: <http://www.isc.org/>

Glossary

A

access control list (ACL)	A software authorization mechanism that enables you to control which users have access to a server. Users can define ACL rules that are specific to a particular file or directory, granting or denying access to one or more users or groups.
Active Directory	A distributed directory service included with Microsoft Windows Server operating systems. It provides both authentication of user credentials and authorization of user access levels to networked resources.
actual power	The amount of power consumed by all power supplies in the system.
address	In networking, a unique code that identifies a node in the network. Names such as "host1.companyname.com" are translated to dotted-quad addresses, such as "168.124.3.4" by the Domain Name Service (DNS).
address resolution	A means for mapping Internet addresses into physical media access control (MAC) addresses or domain addresses.
Address Resolution Protocol (ARP)	A protocol used to associate an Internet Protocol (IP) address with a network hardware address (MAC address).
Administrator	The person with full access (root) privileges to the managed host system.
agent	A software process, usually corresponding to a particular local managed host, that carries out manager requests and makes local system and application information available to remote users.
alert	A message or log generated by the collection and analysis of error events. An alert indicates that there is a need to perform some hardware or software corrective action.
Alert Standard Format (ASF)	A preboot or out-of-band platform management specification that enables a device, such as an intelligent Ethernet controller, to autonomously scan ASF-compliant sensors on the motherboard for voltage, temperature, or other excursions and to send Remote Management and Control Protocol

(RMCP) alerts according to the Platform Event Trap (PET) specification. ASF was intended primarily for out-of-band management functions for client desktops. ASF is defined by the Distributed Management Task Force (DMTF).

authentication	The process that verifies the identity of a user in a communication session, or a device or other entity in a computer system, before that user, device, or other entity can access system resources. Session authentication can work in two directions. A server authenticates a client to make access-control decisions. The client can authenticate the server as well. With Secure Sockets Layer (SSL), the client always authenticates the server.
authenticated user	A user that has successfully undergone the process of authentication and has subsequently been granted access privileges to particular system resources.
authorization	The process of granting specific access privileges to a user. Authorization is based on authentication and access control.
available power	On a rackmounted server, available power is the sum of all the power that the power supplies can provide. On a server module, available power is the amount of power the chassis is willing to provide to the server module.

B

bandwidth	A measure of the volume of information that can be transmitted over a communication link. Often used to describe the number of bits per second a network can deliver.
baseboard management controller (BMC)	A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The BMC provides another interface to the system event log (SEL). Typical functions of the BMC are to measure processor temperature, power supply values, and cooling fan status. The BMC can take autonomous action to preserve system integrity.
baud rate	The rate at which information is transmitted between devices, for example, between a terminal and a server.
bind	In the Lightweight Directory Access Protocol (LDAP), this refers to the authentication process that LDAP requires when users access the LDAP directory. Authentication occurs when the LDAP client binds to the LDAP server.
BIOS (Basic Input/Output System)	System software that controls the loading of the operating system and testing of hardware at system power on. BIOS is stored in read-only memory (ROM).

bits per second (bps) The unit of measurement for data transmission speed.

boot loader A program contained in read-only memory (ROM) that automatically runs at system power-on to control the first stage of system initialization and hardware tests. The boot loader then transfers control to a more complex program that loads the operating system.

C

cache A copy of original data that is stored locally, often with instructions or the most frequently accessed information. Cached data does not have to be retrieved from a remote server again when requested. A cache increases effective memory transfer rates and processor speed.

certificate Public key data assigned by a trusted Certificate Authority (CA) to provide verification of an entity's identity. This is a digitally signed document. Both clients and servers can have certificates. Also called a "public key certificate."

Certificate Authority (CA) A trusted organization that issues public key certificates and provides identification to the owner of the certificate. A public key Certificate Authority issues certificates that state a relationship between an entity named in the certificate, and a public key that belongs to that entity, which is also present in the certificate.

chassis monitoring module (CMM) A typically redundant, hot-pluggable module that works with the service processor (SP) on each blade to form a complete chassis management system.

client In the client/server model, a system or software on a network that remotely accesses resources of a server on a network.

command-line interface (CLI) A text-based interface that enables users to type executable instructions at a command prompt.

console A terminal, or dedicated window on a screen, where system messages are displayed. The console window enables you to configure, monitor, maintain, and troubleshoot many server software components.

Coordinated Universal Time (UTC) The international standard for time. UTC was formerly called Greenwich Meridian Time (GMT). UTC is used by Network Time Protocol (NTP) servers to synchronize systems and devices on a network.

core file A file created by the Solaris or Linux operating system when a program malfunctions and terminates. The core file holds a snapshot of memory, taken at the time the fault occurred. Also called a "crash dump file."

critical event	A system event that seriously impairs service and requires immediate attention.
customer-replaceable unit (CRU)	A system component that the user can replace without special training or tools.

D

Data Encryption Standard (DES)	A common algorithm for encrypting and decrypting data.
Desktop Management Interface (DMI)	A specification that sets standards for accessing technical support information about computer hardware and software. DMI is hardware and operating system (OS) independent, and can manage workstations, servers, or other computing systems. DMI is defined by the Distributed Management Task Force (DMTF).
digital signature	A certification of the source of digital data. A digital signature is a number derived from a public key cryptographic process. If the data is modified after the signature was created, the signature becomes invalid. For this reason, a digital signature can ensure data integrity and detection of data modification.
Digital Signature Algorithm (DSA)	A cryptographic algorithm specified by the Digital Signature Standard (DSS). DSA is a standard algorithm used to create digital signatures.
direct memory access (DMA)	The transfer of data directly into memory without supervision of the processor.
directory server	In the Lightweight Directory Access Protocol (LDAP), a server which stores and provides information about people and resources within an organization from a logically centralized location.
Distinguished Name (DN)	In the Lightweight Directory Access Protocol (LDAP), a unique text string that identifies an entry's name and location within the directory. A DN can be a fully qualified domain name (FQDN) that includes the complete path from the root of the tree.
Distributed Management Task Force (DMTF)	A consortium of over 200 companies that authors and promotes standards for the purpose of furthering the ability to remotely manage computer systems. Specifications from the DTMF include the Desktop Management Interface (DMI), the Common Information Model (CIM), and the Alert Standard Format (ASF).

domain	A grouping of hosts that is identified by a name. The hosts usually belong to the same Internet Protocol (IP) network address. The domain also refers to the last part of a fully qualified domain name (FQDN) that identifies the company or organization that owns the domain. For example, "oracle.com" identifies Oracle Corporation as the owner of the domain.
domain name	The unique name assigned to a system or group of systems on the Internet. The host names of all the systems in the group have the same domain name suffix, such as "oracle.com." Domain names are interpreted from right to left. For example, "oracle.com" is both the domain name of Oracle Corporation, and a subdomain of the top-level ".com" domain.
Domain Name Server (DNS)	The server that typically manages host names in a domain. DNS servers translate host names, such as "www.example.com," into Internet Protocol (IP) addresses, such as "030.120.000.168."
Domain Name System (DNS)	A distributed name resolution system that enables computers to locate other computers on a network or the Internet by domain name. The system associates standard Internet Protocol (IP) addresses, such as "00.120.000.168," with host names, such as "www.oracle.com." Machines typically get this information from a DNS server.
Dynamic Domain Name Service (DDNS)	A service that ensures that a Domain Name Server (DNS) always knows the dynamic or static IP address associated with a domain name.
Dynamic Host Configuration Protocol (DHCP)	A protocol that enables a DHCP server to assign Internet Protocol (IP) addresses dynamically to systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

E

enhanced parallel port (EPP)	A hardware and software standard that enables systems to transmit data at twice the speed of standard parallel ports.
Ethernet	An industry-standard type of local area network (LAN) that enables real-time communication between systems connected directly through cables. Ethernet uses a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) algorithm as its access method, wherein all nodes listen for, and any node can begin transmitting data. If multiple nodes attempt to transmit at the same time (a collision), the transmitting nodes wait for a random time before attempting to transmit again.
event	A change in the state of a managed object. The event-handling subsystem can provide a notification to which a software system must respond when it occurs, but which the software did not solicit or control.
external serial port	The RJ-45 serial port on the server.

externally initiated reset (XIR) A signal that sends a “soft” reset to the processor in a domain. XIR does not reboot the domain. An XIR is generally used to escape from a hung system in order to reach the console prompt. A user can then generate a core dump file, which can be useful in diagnosing the cause of the hung system.

F

failover The automatic transfer of a computer service from one system, or more often a subsystem, to another to provide redundant capability.

Fast Ethernet Ethernet technology that transfers data up to 100M bits per second. Fast Ethernet is backward-compatible with 10M-bit per second Ethernet installations.

Fault Management Architecture (FMA) An architecture that ensures a computer can continue to function despite a hardware or software failure.

field-replaceable unit (FRU) A system component that is replaceable at the customer site.

file system A consistent method by which information is organized and stored on physical media. Different operating systems typically have different file systems. File systems are often a tree-structured network of files and directories, with a root directory at the top and parent and child directories below root.

File Transfer Protocol (FTP) A basic Internet protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP) that enables the retrieving and storing of files between systems on the Internet without regard for the operating systems or architectures of the systems involved in the file transfer.

firewall A network configuration, usually both hardware and software, that protects networked computers within an organization from outside access. A firewall can monitor or prohibit connections to and from specified services or hosts.

firmware Software that is typically used to help with the initial booting stage of a system and with system management. Firmware is embedded in read-only memory (ROM) or programmable ROM (PROM).

fully qualified domain name (FQDN) The complete and unique Internet name of a system, such as “www.oracle.com.” The FQDN includes a host server name (www) and its top-level (.com) and second-level (.oracle) domain names. An FQDN can be mapped to a system’s Internet Protocol (IP) address.

G

gateway	A computer or program that interconnects two networks and then passes data packets between the networks. A gateway has more than one network interface.
Gigabit Ethernet	Ethernet technology that transfers data up to 1000M bits per second.
graphical user interface (GUI)	An interface that uses graphics, along with a keyboard and mouse, to provide easy-to-use access to an application.

H

host	A system, such as a backend server, with an assigned Internet Protocol (IP) address and host name. The host is accessed by other remote systems on the network.
host ID	Part of the 32-bit Internet Protocol (IP) address used to identify a host on a network.
host name	The name of a particular machine within a domain. Host names always map to a specific Internet Protocol (IP) address.
hot-plug	Describes a component that is safe to remove or add while the system is running. However, before removing the component, the system administrator must prepare the system for the hot-plug operation. After the new component is inserted, the system administrator must instruct the system to reconfigure the device into the system.
hot-swap	Describes a component that can be installed or removed by simply pulling the component out and putting a new component into a running system. The system either automatically recognizes the component change and configures it or requires user interaction to configure the system. However, in neither case is a reboot required. All hot-swappable components are hot pluggable, but not all hot-pluggable components are hot-swappable.
Hypertext Transfer Protocol (HTTP)	The Internet protocol that retrieves hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client. HTTP is based on Transmission Control Protocol/Internet Protocol (TCP/IP).
Hypertext Transfer Protocol Secure (HTTPS)	An extension of HTTP that uses Secure Sockets Layer (SSL) to enable secure transmissions over a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

I

in-band system management	Server management capability that is enabled only when the operating system is initialized and the server is functioning properly.
Integrated Lights Out Manager (ILOM)	An integrated hardware, firmware, and software solution for in-chassis or in-blade system management.
Intelligent Platform Management Interface (IPMI)	A hardware-level interface specification that was designed primarily for out-of-band management of server systems over a number of different physical interconnects. The IPMI specification describes extensive abstractions regarding sensors. This enables a management application running on the operating system (OS) or in a remote system to comprehend the environmental makeup of the system and to register with the system's IPMI subsystem to receive events. IPMI is compatible with management software from heterogeneous vendors. IPMI functionality includes Field Replacable Unit (FRU) inventory reporting, system monitoring, logging, system recovery (including local and remote system resets and power on and off capabilities), and alerting.
internal serial port	The connection between the host server and Oracle ILOM that enables an Oracle ILOM user to access the host serial console. The Oracle ILOM internal serial port speed must match the speed of the serial console port on the host server, often referred to as serial port 0, COM1, or /dev/ttyS0. Normally, the host serial console settings match Oracle ILOM's default settings (9600 baud, 8N1 [eight data bits, no parity, one stop bit], no flow control).
Internet Control Message Protocol (ICMP)	An extension to the Internet Protocol (IP) that provides for routing, reliability, flow control, and sequencing of data. ICMP specifies error and control messages used with the IP.
Internet Protocol (IP)	The basic network layer protocol of the Internet. IP enables the unreliable delivery of individual packets from one host to another. IP does not guarantee that the packet will be delivered, how long it will take, or if multiple packets will be delivered in the order they were sent. Protocols layered on top of IP add connection reliability.
Internet Protocol (IP) address	In Transmission Control Protocol/Internet Protocol (TCP/IP), a unique 32-bit number that identifies each host or other hardware system on a network. The IP address is a set of numbers separated by dots, such as "192.168.255.256," which specifies the actual location of a machine on an intranet or the Internet.
IPMItool	A utility used to manage IPMI-enabled devices. IPMItool can manage IPMI functions of either the local system or a remote system. Functions include managing field-replaceable unit (FRU) information, local area network (LAN) configurations, sensor readings, and remote system power control.

J

Java Remote Console

A console written in Java that allows a user to access an application while it is running.

Java(TM) Web Start application

A web application launcher. With Java Web Start, applications are launched by clicking on the web link. If the application is not present on your system, Java Web Start downloads it and caches it onto your system. Once an application is downloaded to its cache, it can be launched from a desktop icon or browser

K

kernel

The core of the operating system (OS) that manages the hardware and provides fundamental services, such as filing and resource allocation, that the hardware does not provide.

Keyboard Controller Style (KCS) interface

A type of interface implemented in legacy personal computer (PC) keyboard controllers. Data is transferred across the KCS interface using a per-byte handshake.

keyboard, video, mouse, storage (KVMS)

A series of interfaces that enables a system to respond to keyboard, video, mouse, and storage events.

L

lights out management (LOM)

Technology that provides the capability for out-of-band communication with the server even if the operating system is not running. This enables the system administrator to switch the server on and off; view system temperatures, fan speeds, and so forth; and restart the system from a remote location.

Lightweight Directory Access Protocol (LDAP)

A directory service protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data. LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP) and across multiple platforms.

Lightweight Directory Access Protocol (LDAP) server

A software server that maintains an LDAP directory and service queries to the directory. The Oracle Sun Directory Services and the Netscape Directory Services are implementations of an LDAP server.

local area network (LAN)	A group of systems in close proximity that can communicate via connecting hardware and software. Ethernet is the most widely used LAN technology.
local host	The processor or system on which a software application is running.

M

major event	A system event that impairs service, but not seriously.
Management Information Base (MIB)	A tree-like, hierarchical system for classifying information about resources in a network. The MIB defines the variables that the master Simple Network Management Protocol (SNMP) agent can access. The MIB provides access to the server's network configuration, status, and statistics. Using SNMP, you can view this information from a network management station (NMS). By industry agreement, individual developers are assigned portions of the tree structure to which they may attach descriptions that are specific to their own devices.
man pages	Online UNIX documentation.
media access control (MAC) address	Worldwide unique, 48-bit, hardware address number that is programmed in to each local area network interface card (NIC) at the time of manufacture.
Message Digest 5 (MD5)	A secure hashing function that converts an arbitrarily long data string into a short digest of data that is unique and of fixed size.
minor event	A system event that does not currently impair service, but which needs correction before it becomes more severe.

N

namespace	In the tree structure of a Lightweight Directory Access Protocol (LDAP) directory, a set of unique names from which an object name is derived and understood. For example, files are named within the file namespace and printers are named within the printer namespace.
Network File System (NFS)	A protocol that enables disparate hardware configurations to function together transparently.
Network Information Service (NIS)	A system of programs and data files that UNIX systems use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computer systems.

network interface card (NIC)	An internal circuit board or card that connects a workstation or server to a networked device.
network management station (NMS)	A powerful workstation with one or more network management applications installed. The NMS is used to remotely manage a network.
network mask	A number used by software to separate the local subnet address from the rest of a given Internet Protocol (IP) address.
Network Time Protocol (NTP)	An Internet standard for Transmission Control Protocol/Internet Protocol (TCP/IP) networks. NTP synchronizes the clock times of networked devices with NTP servers to the millisecond using Coordinated Universal Time (UTC).
node	An addressable point or device on a network. A node can connect a computing system, a terminal, or various peripheral devices to the network.
nonvolatile memory	A type of memory that ensures that data is not lost when system power is off.

O

object identifier (OID)	A number that identifies an object's position in a global object registration tree. Each node of the tree is assigned a number, so that an OID is a sequence of numbers. In Internet usage the OID numbers are delimited by dots, for example, "0.128.45.12." In the Lightweight Directory Access Protocol (LDAP), OIDs are used to uniquely identify schema elements, including object classes and attribute types.
OpenBoot(TM) PROM	A layer of software that takes control of an initialized system after the power-on self-test (POST) successfully tests components. OpenBoot PROM builds data structures in memory and boots the operating system.
OpenIPMI	An operating system-independent, event-driven library for simplifying access to the Intelligent Platform Management Interface (IPMI).
Operator	A user with limited privileges to the managed host system.
out-of-band (OOB) system management	Server management capability that is enabled when the operating system network drivers or the server are not functioning properly.

P

parity	A method used by a computer for checking that data received matches data sent. Also refers to information stored with data on a disk that enables the controller to rebuild data after a drive failure.
Pc-Check	An application made by Eurosoft (UK) Ltd. that runs diagnostic tests on computer hardware.
permissions	A set of privileges granted or denied to a user or group that specify read, write, or execution access to a file or directory. For access control, permissions state whether access to the directory information is granted or denied, and the level of access that is granted or denied.
permitted power	The maximum power that the server will permit to be used at any given time.
physical address	An actual hardware address that matches a memory location. Programs that refer to virtual addresses are subsequently mapped to physical addresses.
Platform Event Filtering (PEF)	A mechanism that configures the service processor to take selected actions when it receives event messages, for example, powering off or resetting the system or triggering an alert.
Platform Event Trap (PET)	A configured alert triggered by a hardware or firmware (BIOS) event. A PET is an Intelligent Platform Management Interface (IPMI)-specific, Simple Network Management Protocol (SNMP) trap, which operates independently of the operating system.
port	The location (socket) to which Transmission Control Protocol/Internet Protocol (TCP/IP) connections are made. Web servers traditionally use port 80, the File Transfer Protocol (FTP) uses port 21, and Telnet uses port 23. A port enables a client program to specify a particular server program in a computer on a network. When a server program is started initially, it binds to its designated port number. Any client that wants to use that server must send a request to bind to the designated port number.
port number	A number that specifies an individual Transmission Control Protocol/Internet Protocol (TCP/IP) application on a host machine, providing a destination for transmitted data.
power cycling	The process of turning the power to a system off then on again.
Power Monitoring interface	An interface that enables a user to monitor real-time power consumption, including available power, actual power, and permitted power, for the service processor (SP) or an individual power supply with accuracy to within one minute of the time the power usage occurred.

power-on self-test (POST)	A program that takes uninitialized system hardware and probes and tests its components at system startup. POST configures useful components into a coherent, initialized system and hands it over to the OpenBoot PROM. POST passes to OpenBoot PROM a list of only those components that have been successfully tested.
Preboot Execution Environment (PXE)	An industry-standard client/server interface that enables a server to boot an operating system (OS) over a Transmission Control Protocol/Internet Protocol (TCP/IP) network using Dynamic Host Configuration Protocol (DHCP). The PXE specification describes how the network adapter card and BIOS work together to provide basic networking capabilities for the primary bootstrap program, enabling it to perform a secondary bootstrap over the network, such as a TFTP load of an OS image. Thus, the primary bootstrap program, if coded to PXE standards, does not need knowledge of the system's networking hardware.
Privacy Enhanced Mail (PEM) protocol	A standard for Internet electronic mail that encrypts data to ensure privacy and data integrity.
proxy	A set of rules that describes how systems or devices on a network exchange information.
public key encryption	A mechanism whereby one system acts on behalf of another system in responding to protocol requests.
	A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt messages, the recipients use their unpublished private keys, which are known only to them. Knowing the public key does not enable users to deduce the corresponding private key.

R

real-time clock (RTC)	A battery-backed component that maintains the time and date for a system, even when the system is powered off.
reboot	An operating system-level operation that performs a system shutdown followed by a system boot. Power is a prerequisite.
redirection	The channeling of input or output to a file or device rather than to the standard input or output of a system. The result of redirection sends input or output that a system would normally display to the display of another system.
Remote Authentication Dial-In User Service (RADIUS)	A protocol that authenticates users against information in a database on a server and grants authorized users access to a resource.

Remote Management and Control Protocol (RMCP)	A networking protocol that enables an administrator to respond to an alert remotely by powering the system on or off or forcing a reboot.
remote procedure call (RPC)	A method of network programming that enables a client system to call functions on a remote server. The client starts a procedure at the server and the result is transmitted back to the client.
remote system	A system other than the one on which the user is working.
reset	A hardware-level operation that performs a system power-off, followed by a system power-on.
role	An attribute of user accounts that determines user access rights.
root	In UNIX operating systems, the name of the superuser (root). The root user has permissions to access any file and carry out other operations not permitted to ordinary users. Roughly equivalent to the Administrator user name on Windows Server operating systems.
root directory	The base directory from which all other directories stem, either directly or indirectly.
router	A system that assigns a path over which to send network packets or other Internet traffic. Although both hosts and gateways do routing, the term “router” commonly refers to a device that connects two networks.
RSA algorithm	A cryptographic algorithm developed by RSA Data Security, Inc. It can be used for both encryption and digital signatures.
schema	Definitions that describe what type of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.

S

Secure Shell (SSH)	A UNIX shell program and network protocol that enables secure and encrypted log in and execution of commands on a remote system over an insecure network.
Secure Socket Layer (SSL)	A protocol that enables client-to-server communication on a network to be encrypted for privacy. SSL uses a key exchange method to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. SSL creates a secure connection between a web server and a web client. Hypertext Transfer Protocol Secure (HTTPS) uses SSL.

sensor data record (SDR)	To facilitate dynamic discovery of features, the Intelligent Platform Management Interface (IPMI) includes this set of records. They include software information, such as how many sensors are present, what type they are, their events, threshold information, and so on. The sensor data records enable software to interpret and present sensor data without any prior knowledge about the platform.
serial console	A terminal or a tip line connected to the serial port on the service processor. A serial console is used to configure the system to perform other administrative tasks.
serial port	A port that provides access to the command-line interface (CLI) and the system console stream using serial port redirection.
server certificate	A certificate used with Hypertext Transfer Protocol Secure (HTTPS) to authenticate web applications. The certificate can be self-signed or issued by a Certificate Authority (CA).
Server Message Block (SMB) protocol	A network protocol that enables files and printers to be shared across a network. The SMB protocol provides a method for client applications to read and write to files on and request services from server programs in the network. The SMB protocol enables you to mount file systems between Windows and UNIX systems. The SMB protocol was designed by IBM and subsequently modified by Microsoft Corp. Microsoft renamed the protocol the Common Internet File System (CIFS).
service processor (SP)	A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The SP provides another interface to the system event log (SEL). Typical functions of the SP are to measure processor temperature, power supply values, and cooling fan status. The SP can take autonomous action to preserve system integrity.
session time-out	A specified duration after which a server can invalidate a user session.
Simple Mail Transfer Protocol (SMTP)	A Transmission Control Protocol/Internet Protocol (TCP/IP) used for sending and receiving email.
Simple Network Management Protocol (SNMP)	A simple protocol used to exchange data about network activity. With SNMP, data travels between a managed device and a network management station (NMS). A managed device can be any device that runs SNMP, such as hosts, routers, web servers, or other servers on the network.
Single Sign On (SSO)	A form of authentication in which a user enters credentials once to access multiple applications.
Snapshot utility	An application that collects data about the state of the server processor (SP). Oracle Services uses this data for diagnostic purposes.

subnet	A working scheme that divides a single logical network into smaller physical networks to simplify routing. The subnet is the portion of an Internet Protocol (IP) address that identifies a block of host IDs.
subnet mask	A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Also called an “address mask.”
Sun Blade Modular System	A chassis that holds multiple Sun Blade server modules.
Sun Blade server module	A server module (blade) that can be plugged into a chassis, also known as a modular system
Sun Oracle ILOM Remote Console	A graphical user interface that enables a user to redirect devices (keyboard, mouse, video display, storage media) from a desktop to a remote host server.
superuser	A special user who has privileges to perform all administrative functions on a UNIX system. Also called “root.”
syslog	A protocol over which log messages can be sent to a server.
system event log (SEL)	A log that provides nonvolatile storage for system events that are logged autonomously by the service processor or directly with event messages sent from the host.
system identifier	A text string that helps identify the host system. This string is included as a varbind in SNMP traps generated from the SUN-HW-TRAP-MIB. While the system identifier can be set to any string, it is most commonly used to help identify the host system. The host system can be identified by a description of its location or by referencing the host name used by the operating system on the host.



T

Telnet	The virtual terminal program that enables the user of one host to log in to a remote host. A Telnet user of one host who is logged in to a remote host can interact as a normal terminal user of the remote host.
threshold	Minimum and maximum values within a range that sensors use when monitoring temperature, voltage, current, and fan speed.
time-out	A specified time after which the server should stop trying to finish a service routine that appears to be hung.
transmission control block (TCB)	Part of the Transmission Control Protocol/Internet Protocol (TCP/IP) that records and maintains information about the state of a connection.

Transmission Control Protocol/Internet Protocol (TCP/IP)	An Internet protocol that provides for the reliable delivery of data streams from one host to another. TCP/IP transfers data between different types of networked systems, such as systems running Solaris, Microsoft Windows, or Linux software. TCP guarantees delivery of data and that packets will be delivered in the same sequence in which they were sent.
trap	Event notification made by Simple Network Management Protocol (SNMP) agents by their own initiative when certain conditions are detected. SNMP formally defines seven types of traps and permits subtypes to be defined.
Trivial File Transport Protocol (TFTP)	A simple transport protocol that transfers files to systems. TFTP uses User Datagram Protocol (UDP).

U

Uniform Resource Identifier (URI)	A unique string that identifies a resource on the Internet or an intranet.
Universal Serial Bus (USB)	An external bus standard that supports data transfer rates of 450M bits per second (USB 2.0). A USB port connects devices, such as mouse pointers,
user account	A record of essential user information that is stored on the system. Each user who accesses a system has a user account.
User Datagram Protocol (UDP)	A connectionless transport layer protocol that adds some reliability and multiplexing to the Internet Protocol (IP). UDP enables one application program to deliver, via IP, datagrams to another application program on another machine. The Simple Network Management Protocol (SNMP) is usually implemented over UDP.
user privilege levels	An attribute of a user that designates the operations a user can perform and the resources a user can access.
user identification (userid)	A unique string identifying a user to a system.
user identification number (UID number)	The number assigned to each user accessing a UNIX system. The system uses UID numbers to identify, by number, the owners of files and directories.
user name	A combination of letters, and possibly numbers, that identifies a user to the system.

W

web server Software that provides services to access the Internet or an intranet. A web server hosts web sites, provides support for HTTP/HTTPS and other protocols, and executes server-side programs.

wide area network (WAN) A network consisting of many systems that provides file transfer services. A WAN can cover a large physical area, sometimes worldwide.

X

X.509 certificate The most common certificate standard. X.509 certificates are documents containing a public key and associated identity information, digitally signed by a Certificate Authority (CA).

X Window System A common UNIX window system that enables a workstation or terminal to control multiple sessions simultaneously.

Index

A

- Active Directory, 34
 - determining user authorization levels, 35
 - overview, 35
 - user authentication/authorization, 35
- active ILOM sessions supported, 15
- alerts
 - defining an alert rule, 50, 54
 - managing from CLI, 53
 - managing from SNMP host, 55
 - managing from web interface, 54
 - specifying destination, 51
 - types of levels, 52
 - types supported, 49, 51
 - warnings for system failures, 49
- authentication
 - using Active Directory, 34
 - using LDAP, 36
 - using RADIUS, 37
 - using SSH host keys, 34
- available power, 72

B

- BIOS configurations
 - updating, 3

C

- chassis monitoring module (CMM)
 - managing with ILOM, 10
- clock settings, 48
- collecting data for Sun Services, 49
- connecting to ILOM, 14

D

- data network
 - compared to management network, 14

- default user account, 8

DHCP

- lease release, 116
- lease renewal, 116
- uses, 115

- DNS database, 116

- dnssec-keygen, 118

- Domain Name Service (DNS), 115

- downloadable firmware updates, 4

Dynamic DNS

- configuration assumptions, 117
- configuration example, 117
- configuring DHCP and DNS, 117
- Debian r4.0 environment, 117
- dnssec-keygen, 118
- host name, determining, 116
- MAC address-based host names, 116
- operating systems supported, 117
- overview, 115
- transaction, description of, 116
- well-known host name, 115

- Dynamic Domain Name Service

- See Dynamic DNS

- Dynamic Host Configuration Protocol (DHCP)

- uses, 115

E

- Email Notification alerts, 51
- ENTITY-MIB, 10
- Error and fault management, 5
- Ethernet connection to ILOM, 16
- Ethernet management port
 - connecting to ILOM, 15
- event log
 - capturing timestamps, 48
 - types of events displayed, 47

examples, 115

F

fault management
 monitoring and diagnosing hardware, 45
 viewing faulted components, 47
firmware
 updating, 3

H

hardware and FRU inventory, 4
host name
 assigned using DDNS, 14
 assigning, 16
host name format and contents, 115

I

ILOM service processor
 embedded operating system, 2
 management capabilities, 10
init.d script, 119
input power, 71
Integrated Lights Out Manager (ILOM)
 capabilities, 2
 connecting to, 14
 description, 2
 features and functionality, 4
 integrating with other management tools, 3
 interfaces to, 9
 new 3.0 features, 5
 roles assigned to accounts, 32
 system monitoring features, 40
 user interfaces supported, 3, 9
Intelligent Platform Management Interface (IPMI)
 capabilities, 9
interfaces to ILOM, 9
IPMI PET alerts, 51

L

LDAP/SSL
 overview, 36
LEDs
 when illuminated by ILOM, 41
Lightweight Directory Access Protocol (LDAP)
 overview, 36
 used for authentication, 36

log in to ILOM
 using root user account password, 7

M

management network
 compared to data network, 14
 overview, 14
MIBs supported, 9

N

network connection
 using network management port, 14
 using serial management port, 14
network ports used by ILOM, 16
nslookup, 119

O

out-of-band management, 2
output power, 71

P

power monitoring terminology, 71

R

RADIUS
 client-server model, 37
 overview, 37
 used for authentication, 37
remote access, 4
remote hardware monitoring, 4
remote power control
 about, 110
roles for user accounts, 6, 32

S

sensor readings
 monitoring and diagnosing faults, 45
 types of data reported, 41
serial management port
 connecting to ILOM, 16
service processor (SP)
 managing with ILOM, 10
Service Snapshot utility, 49
Simple Network Management Protocol (SNMP)
 capabilities, 9
 configuring alert rules, 54

- MIBs supported, 9
- Single Sign On
 - overview, 33
- SNMP Trap alerts, 51
- SNMP-FRAMEWORK-MIB, 9
- SNMP-MPD-MIB, 10
- SNMPv2-MIB, 10
- SSH key-based authentication, 34
- Sun xVM Ops Center
 - using with ILOM, 3
- SUN-HW-TRAP-MIB, 9
- SUN-ILOM-CONTROL-MIB, 9
- SUN-ILOM-PET-MIB, 9
- SUN-PLATFORM-MIB, 9
- syslog logging utility, 48
- System alerts, 5
- system identifier
 - assigning, 16
- system indicators
 - customer changeable states, 42
 - illuminating conditions, 41
 - states, 41
 - system assigned states, 42
- system monitoring features
 - overview, 40
- system power control and monitoring, 5

T

- third-party management tools, 4

U

- user accounts
 - authentication, 32
 - configuring, 5
 - default user account, 8
 - guidelines for managing, 31
 - number of accounts supported, 32
 - privileges assigned, 32
 - roles assigned, 32
 - root user account, 7
 - specifying names for, 32

W

- web interface capabilities, 9

