

Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 5.0.x



E95139-04
December 2022



Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 5.0.x,

E95139-04

Copyright © 2019, 2022, Oracle and/or its affiliates.

Primary Author: Cheryl Smith, Heidi Hall

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, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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 that 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®, Java, MySQL and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Copyright © 2019, 2022, Oracle et/ou ses affiliés.

Ce logiciel et la documentation connexe sont fournis en vertu d'un contrat de licence assorti de restrictions relatives à leur utilisation et divulgation. Ils sont protégés en vertu des lois sur la propriété intellectuelle. Sauf dispositions contraires prévues de manière expresse dans votre contrat de licence ou permises par la loi, vous ne pouvez pas utiliser, copier, reproduire, traduire, diffuser, modifier, mettre sous licence, transmettre, distribuer, présenter, effectuer, publier ou afficher à toutes fins une partie de ces derniers sous quelque forme que ce soit, par quelque moyen que ce soit. Sont interdits l'ingénierie inverse, le désassemblage ou la décompilation de ce logiciel, sauf à des fins d'interopérabilité selon les dispositions prévues par la loi.

L'information contenue dans les présentes est sujette à changement sans préavis. Nous ne garantissons pas qu'elle est exempte d'erreur. Si vous y relevez des erreurs, veuillez nous les signaler par écrit.

Si ce logiciel, la documentation du logiciel ou les données (comme défini dans la réglementation Federal Acquisition Regulation) ou la documentation afférente sont livrés sous licence au gouvernement des États-Unis d'Amérique ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du gouvernement des États-Unis d'Amérique, la notice suivante s'applique :

UTILISATEURS DE FIN DU GOUVERNEMENT É.-U. : programmes Oracle (y compris tout système d'exploitation, logiciel intégré, tout programme intégré, installé ou activé sur le matériel livré et les modifications de tels programmes) et documentation sur l'ordinateur d'Oracle ou autres logiciels Oracle Les données fournies aux utilisateurs finaux du gouvernement des États-Unis ou auxquelles ils ont accès sont des "logiciels informatiques commerciaux", des "documents sur les logiciels informatiques commerciaux" ou des "données relatives aux droits limités" conformément au règlement fédéral sur l'acquisition applicable et aux règlements supplémentaires propres à l'organisme. À ce titre, l'utilisation, la reproduction, la duplication, la publication, l'affichage, la divulgation, la modification, la préparation des œuvres dérivées et/ou l'adaptation des i) programmes Oracle (y compris tout système d'exploitation, logiciel intégré, tout programme intégré, installé, ou activé sur le matériel livré et les modifications de ces programmes), ii) la documentation informatique d'Oracle et/ou iii) d'autres données d'Oracle, sont assujetties aux droits et aux limitations spécifiés dans la licence contenue dans le contrat applicable. Les conditions régissant l'utilisation par le gouvernement des États-Unis des services en nuage d'Oracle sont définies par le contrat applicable à ces services. Aucun autre droit n'est accordé au gouvernement américain.

Ce logiciel ou matériel informatique est destiné à un usage général, dans diverses applications de gestion de l'information. Il n'a pas été conçu pour être utilisé dans le cadre d'applications dangereuses, y compris des applications susceptibles de causer des blessures corporelles. Si vous utilisez ce logiciel ou matériel informatique dans des applications dangereuses, il vous revient d'adopter les mesures relatives à la protection contre les interruptions, aux copies de sauvegarde et à la redondance ainsi que toute autre mesure visant à garantir son utilisation en toute sécurité. Oracle Corporation et ses sociétés affiliées déclinent toute responsabilité relativement aux dommages pouvant résulter de l'utilisation du logiciel ou du matériel informatique dans des applications dangereuses.

Oracle®, Java, MySQL et NetSuite sont des marques de commerce enregistrées d'Oracle Corporation et/ou de ses sociétés affiliées. Les autres noms ou raisons sociales peuvent être des marques de commerce de leurs propriétaires respectifs.

Intel et Intel Inside sont des marques de commerce ou des marques de commerce enregistrées de Intel Corporation. Toutes les marques de commerce SPARC sont utilisées sous licence et sont des marques de commerce ou des marques de commerce enregistrées de SPARC International, Inc. AMD, Epyc et le logo AMD sont des marques de commerce ou des marques de commerce enregistrées de Advanced Micro Devices. UNIX est une marque de commerce enregistrée de The Open Group.

Ce logiciel ou matériel informatique et sa documentation peuvent fournir de l'information sur du contenu, des produits et des services tiers, ou y donner accès. Oracle Corporation et ses sociétés affiliées déclinent toute responsabilité quant aux garanties de quelque nature que ce soit relatives au contenu, aux produits et aux services offerts par des tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. Oracle Corporation et ses sociétés affiliées ne pourront être tenus responsable des pertes, frais et dommages de quelque nature que ce soit découlant de l'accès à du contenu, des produits ou des services tiers, ou de leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Contents

1 Using This Documentation

Product Documentation Library	1-1
Feedback	1-1

2 Oracle ILOM Overview

Related Information	2-1
About Oracle ILOM	2-1
Related Information	2-1
Oracle ILOM Features and Functionality	2-1
Supported Management Interfaces	2-3
Related Information	2-3
Supported Operating System Web Browsers	2-3
Related Information	2-4
Integration With Other Management Tools	2-4
About Oracle Enterprise Manager Ops Center	2-4

3 Getting Started With Oracle ILOM

Related Information	3-1
Logging In to Oracle ILOM	3-1
Network Requirements for Logging In	3-1
Related Information	3-2
Log In to the Oracle ILOM Web Interface	3-2
Log In to the Oracle ILOM CLI	3-2
Navigating the Web Interface	3-3
Oracle ILOM Web Interface	3-4
Web Interface Navigation Options	3-5
Chassis View for SPARC M8 and M7 Series Systems	3-9
Navigating the Command-Line Interface (CLI) Namespace Targets	3-10
Oracle ILOM CLI Supports Case Insensitive Expressions	3-10
Oracle ILOM CLI Namespace Targets	3-10
Related Information	3-12

CLI Hierarchy for Oracle ILOM 5.0.x Targets	3-12
Managing PDomains From a SPARC Multi-Domain Server	3-13
Related Information	3-13
Navigating Target Properties and Viewing Supported Commands	3-13
Related Information	3-15

4 Viewing System Inventory, Health, and Performing Service and Management Actions

Related Information	4-1
Viewing System Component Inventory and Health Status	4-1
View System-Level Information and Health Status (Web)	4-1
View Subcomponent-Level Information and Health Status (Web)	4-2
View System-Level Identification and Health Status (CLI)	4-3
View Subcomponent-Level Information and Health Status (CLI)	4-4
Health State: Definitions	4-6
Related Information	4-6
Administering Open Problems	4-6
Open Problems Terminology	4-7
View Open Problems Detected on a Managed Device	4-7
Administering Removable Devices on SPARC M-Series Servers	4-8
Manage M-Series Server Removable Devices	4-8
Managing Oracle ILOM Log Entries	4-10
Log Descriptions	4-10
Log Properties	4-11
Log Time Stamps	4-13
View and Clear Log Entries (Web)	4-13
View and Clear Log Entries (CLI)	4-14
Filter Log Entries	4-14
Performing Common System Management Actions	4-16
View and Modify the Device Power State From the Actions Panel (Web)	4-16
View and Modify the Device Locator State From the Actions Panel (Web)	4-17
Update the Device Firmware From the Actions Panel (Web)	4-18
Launch the Remote Console From the Actions Panel (Web)	4-20
Launch the x86 Oracle System Assistant	4-21

5 Applying Host and System Management Actions

Related Information	5-1
Administering Host Management Configuration Actions	5-1

6 Real-Time Power Monitoring Through Oracle ILOM Interfaces

Related Information	6-1
Monitoring Power Consumption	6-1
View Power Consumption Properties for a Managed Device	6-1
Power Consumption Terminology and Properties	6-2
Related Information	6-4
Monitoring Power Allocations	6-4
View the Power Allocation Plan for a Managed Device	6-4
Power Allocation Plan Properties per Managed Device	6-5
Power Allocated Components and Monitoring Considerations	6-7
Analyzing Power Usage Statistics	6-8
Rolling Average Power Statistics Graphs and Metrics	6-9
View Power Statistics Bar Graphs and Metrics	6-9
Comparing Power History Performance	6-9
Power History Graphs and Metrics	6-9
View Power History Graphs and Metrics	6-9

7 Troubleshooting Oracle ILOM Managed Devices

Related Information	7-1
Network Connection Issues: Oracle ILOM Interfaces	7-1
Tools for Observing and Debugging System Behavior	7-2
Enabling and Running Oracle ILOM Diagnostic Tools	7-3
Enabling x86 Diagnostics to Run at Boot	7-3
Selecting a Diagnostic Test Level	7-4
Enable UEFI Diagnostics to Run at Boot (Web)	7-5
Enable PC-Check to Run at Boot (Web)	7-7
Enable UEFI Diagnostics to Run at Boot (CLI)	7-8
Enable PC-Check to Run at Boot (CLI)	7-9
Running the x86 HWDiag Tool within Oracle ILOM Diag Shell	7-9
Run x86 HWdiag Tool (CLI)	7-10
Generating x86 Processor Interrupt: Debugging System Status	7-10
Generate a Nonmaskable Interrupt	7-11
Enabling Diagnostics to Run at Boot on Legacy SPARC Servers (M6, M5, T5, and Earlier)	7-11
Enable Host Diagnostics to Run on Legacy SPARC Servers (Web)	7-11
Enable Host Diagnostics to Run on Legacy SPARC Servers (CLI)	7-13
Enabling Diagnostics to Run at Boot on Newer SPARC Systems (M7 and T7 Servers)	7-14

Enable Host Diagnostics to Run on Newer SPARC Systems (Web)	7-14
Enable Host Diagnostics to Run on Newer SPARC Systems (CLI)	7-15
Enable SP Diagnostics to Run on Newer SPARC Systems (Web)	7-17
Taking a Snapshot: Oracle ILOM SP State	7-18
Take a Snapshot of the Oracle ILOM SP State (Web)	7-18
Take a Snapshot of the Oracle ILOM SP State (CLI)	7-20
Decrypt an Encrypted Snapshot Output File	7-21
Transfer Snapshot Output to Remote Console Over SSH Connection	7-22

8 Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell

Related Information	8-1
Protecting Against Hardware Faults: Oracle ILOM Fault Manager	8-1
Hardware Fault Notifications	8-1
Hardware Fault Corrective Action	8-2
Fault Events Cleared: Repaired Hardware	8-2
Oracle ILOM Fault Management Shell	8-2
Fault Management Terminology	8-3
Launch a Fault Management Shell Session (CLI)	8-4
Using fmadm to Administer Active Oracle Hardware Faults	8-5
View Information About Active Faulty Components (fmadm faulty)	8-5
Clearing Faults for Repairs or Replacements	8-6
fmadm Command Usage and Syntax	8-6
Clear Faults for Undetected Replaced or Repaired Hardware Components	8-7
Using fmdump to View Historical Fault Management Logs	8-8
Log File Display Commands and Log Descriptions	8-8
View Fault Management Log Files (fmdump)	8-9
Using fmstat to View the Fault Management Statistics Report	8-10
fmstat Report Example and Description	8-10
fmstat Report Example	8-10
fmstat Report Property Descriptions	8-11
View the Fault Management Statistics Report (fmstat)	8-11

9 Using the Command-Line Interface

Related Information	9-1
About the Command-Line Interface (CLI)	9-1
Related Information	9-1
CLI Reference for Supported DMTF Syntax, Command Verbs, and Options	9-2
Supported CLI Syntax	9-2

Related Information	9-3
Basic CLI Commands and Options	9-3
Related Information	9-4
Basic Command-Line Editing Keystrokes	9-5
Related Information	9-6
CLI Reference for Executing Commands to Change Properties	9-6
Executing Commands to Change Target Properties	9-6
Related Information	9-7
Executing Commands That Require Confirmation	9-8
Related Information	9-9
CLI Device Management Namespace Summary	9-9
Related Information:	9-11
CLI Reference for Mapping Management Tasks to CLI Targets	9-11
Management Connection Tasks and Applicable CLI Targets	9-11
Related Information	9-13
Network Deployment Tasks and Applicable CLI Targets	9-14
Related Information	9-15
User Management Tasks and Applicable CLI Targets	9-15
Related Information	9-16
System Power-On Policy Tasks and Applicable CLI Targets	9-16
Related Information	9-17
System Power Usage Policy Tasks and Applicable CLI Targets	9-17
Related Information	9-18
Firmware Update Tasks and Applicable CLI Targets	9-18
Related Information	9-19
Firmware Back Up and Restore Tasks and Applicable CLI Targets	9-20
Related Information	9-20
x86 BIOS Back up and Restore Tasks and Applicable CLI Targets	9-21
Related Information	9-21
System Health Status Tasks and Applicable CLI Targets	9-21
Related Information	9-22
Event, Audit, and System Log Tasks and Applicable CLI Targets	9-22
Related Information	9-22
Alert Notification Tasks and Applicable CLI Targets	9-23
Related Information	9-23
Host Management Tasks and Applicable CLI Targets	9-23
Related Information	9-24
Remote KVMS Service State Tasks and Applicable CLI Target	9-24
Related Information	9-25
Host Serial Console Session Tasks and Applicable CLI Target	9-25
Related Information	9-26

Host Diagnostic Tasks and Applicable CLI Targets	9-26
Related Information	9-27
Fault Management Shell Session Task and Applicable CLI Target	9-27
Related Information	9-27
CLI Legacy Service State Tasks and Applicable CLI Targets	9-28

10 Glossary

A	10-1
access control list (ACL)	10-1
Active Directory	10-1
actual power consumption	10-1
address	10-1
address resolution	10-1
Address Resolution Protocol (ARP)	10-1
Administrator	10-1
agent	10-2
alert	10-2
Alert Standard Format (ASF)	10-2
allocated power	10-2
audit log	10-2
authentication	10-2
authenticated user	10-2
authorization	10-2
available power	10-3
B	10-3
bandwidth	10-3
baseboard management controller (BMC)	10-3
baud rate	10-3
bind	10-3
BIOS (Basic Input/Output System)	10-3
bits per second (bps)	10-3
boot loader	10-3
C	10-4
cache	10-4
certificate	10-4
Certificate Authority (CA)	10-4
client	10-4
command-line interface (CLI)	10-4
Common Information Model (CIM)	10-4
console	10-4

Coordinated Universal Time (UTC)	10-5
core file	10-5
critical event	10-5
customer-replaceable unit (CRU)	10-5
D	10-5
Data Encryption Standard (DES)	10-5
Desktop Management Interface (DMI)	10-5
digital signature	10-5
Digital Signature Algorithm (DSA)	10-5
direct memory access (DMA)	10-5
directory server	10-6
Distinguished Name (DN)	10-6
Distributed Management Task Force (DMTF)	10-6
domain	10-6
domain name	10-6
domain name server (DNS)	10-6
domain name system (DNS)	10-6
dynamic domain name service (DDNS)	10-7
Dynamic Host Configuration Protocol (DHCP)	10-7
E	10-7
enhanced parallel port (EPP)	10-7
Ethernet	10-7
event	10-7
event log	10-7
exhaust temperature	10-7
external serial port	10-7
externally initiated reset (XIR)	10-8
F	10-8
failover	10-8
Fast Ethernet	10-8
fault	10-8
Fault Management Architecture (FMA)	10-8
Fault Manager	10-8
Fault Manager shell	10-8
faulted state	10-8
field-replaceable unit (FRU)	10-8
file system	10-9
File Transfer Protocol (FTP)	10-9
firewall	10-9
firmware	10-9
fully qualified domain name (FQDN)	10-9

G	10-9
gateway	10-9
Gigabit Ethernet	10-9
graphical user interface (GUI)	10-9
H	10-10
health status states	10-10
host	10-10
host ID	10-10
host name	10-10
hot-plug	10-10
hot-swap	10-10
Hypertext Transfer Protocol (HTTP)	10-10
Hypertext Transfer Protocol Secure (HTTPS)	10-10
I	10-11
in-band system management	10-11
inlet air temperature	10-11
installed hardware minimum	10-11
Intelligent Platform Management Interface (IPMI)	10-11
internal serial port	10-11
Internet Control Message Protocol (ICMP)	10-11
Internet Protocol (IP)	10-11
Internet Protocol (IP) address	10-12
input power	10-12
IPMItool	10-12
J	10-12
Java Remote Console	10-12
Java Web Start application	10-12
K	10-12
kernel	10-12
Keyboard Controller Style (KCS) interface	10-12
keyboard, video, mouse, storage (KVMS)	10-13
L	10-13
lights out management (LOM)	10-13
Lightweight Directory Access Protocol (LDAP)	10-13
Lightweight Directory Access Protocol (LDAP) server	10-13
local area network (LAN)	10-13
local host	10-13
M	10-13
major event	10-13
Management Information Base (MIB)	10-13
maximum permitted power	10-14

man pages	10-14
media access control (MAC) address	10-14
Message Digest 5 (MD5)	10-14
minor event	10-14
N	10-14
namespace	10-14
Network File System (NFS)	10-14
Network Information Service (NIS)	10-14
network interface card (NIC)	10-14
network management station (NMS)	10-15
network mask	10-15
Network Time Protocol (NTP)	10-15
node	10-15
nonvolatile memory	10-15
notification threshold	10-15
O	10-15
object identifier (OID)	10-15
OpenBoot PROM	10-15
OpenIPMI	10-16
open problem	10-16
Operator	10-16
Oracle ILOM Remote System Console (Plus)	10-16
out-of-band (OOB) system management	10-16
output power	10-16
P	10-16
parity	10-16
Pc-Check	10-16
peak permitted	10-16
permissions	10-17
permitted power consumption	10-17
physical address	10-17
Platform Event Filtering (PEF)	10-17
Platform Event Trap (PET)	10-17
port	10-17
port number	10-17
power allocation plan	10-17
power consumption	10-17
power cycling	10-18
power supply maximum	10-18
Power Monitoring interface	10-18
power-on self-test (POST)	10-18

Preboot Execution Environment (PXE)	10-18
Privacy Enhanced Mail (PEM)	10-18
protocol	10-18
proxy	10-18
public key encryption	10-19
R	10-19
rackmount server power consumption	10-19
real-time clock (RTC)	10-19
real-time power monitoring	10-19
reboot	10-19
redirection	10-19
Remote Authentication Dial-In User Service (RADIUS)	10-19
Remote Management and Control Protocol (RMCP)	10-19
remote procedure call (RPC)	10-19
remote system	10-20
reset	10-20
role	10-20
root	10-20
root directory	10-20
router	10-20
RSA algorithm	10-20
S	10-20
schema	10-20
Secure Shell (SSH)	10-20
Secure Sockets Layer (SSL)	10-21
sensor data record (SDR)	10-21
serial console	10-21
serial port	10-21
server certificate	10-21
Server Message Block (SMB) protocol	10-21
service processor (SP)	10-21
session time-out	10-22
Simple Mail Transfer Protocol (SMTP)	10-22
Simple Network Management Protocol (SNMP)	10-22
Single Sign On (SSO)	10-22
Snapshot utility	10-22
subnet	10-22
subnet mask	10-22
superuser	10-22
syslog	10-22
system log	10-23

system identifier	10-23
T	10-23
target	10-23
target limit	10-23
target namespace	10-23
Telnet	10-23
threshold	10-23
time-out	10-23
transmission control block (TCB)	10-24
Transmission Control Protocol/Internet Protocol (TCP/IP)	10-24
trap	10-24
Trivial File Transport Protocol (TFTP)	10-24
U	10-24
uniform resource identifier (URI)	10-24
Universal Serial Bus (USB)	10-24
user account	10-24
User Datagram Protocol (UDP)	10-24
user privilege levels	10-25
user identification (userid)	10-25
user identification number (UID number)	10-25
user name	10-25
W	10-25
web server	10-25
wide area network (WAN)	10-25
X	10-25
X.509 certificate	10-25
X Window System	10-25

Index

1

Using This Documentation

- **Overview** – The guide provides conceptual and procedural information about using the Oracle Integrated Lights Out Manager (ILOM) 4.0.x web and command-line interfaces.
- **Audience** – This guide is intended for technicians, system administrators, and authorized Oracle service providers.
- **Required knowledge** – Users should have experience managing system hardware.

Product Documentation Library

Documentation and resources for this product and related products are available at http://docs.oracle.com/cd/E95134_01/index.html .

Feedback

Provide feedback about this documentation at <http://www.oracle.com/goto/docfeedback> .

2

Oracle ILOM Overview

Related Information

- [SNMP Overview](#)
- [Server Management Using IPMI](#)

About Oracle ILOM

Oracle Integrated Lights Out Manager (ILOM) provides advanced service processor (SP) hardware and software that you can use to manage and monitor your Oracle hardware. Oracle ILOM arrives pre-installed on all of Oracle servers. It is a vital management tool in the data center and can be integrated with other supported third-party system management tools.

Oracle ILOM enables you to experience a single, consistent, and standards-based service processor across all Oracle servers. This means you will have:

- Single, consistent system management interfaces for operators
- Support for rich and standard protocol
- Third-party management tools and interfaces
- Integrated system management functions at no extra cost

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. Oracle ILOM automatically initializes as soon as power is applied to the server. It provides a full-featured, browser-based web interface and has an equivalent command-line interface (CLI). Support for SNMP and IPMI interfaces are also available.

Related Information

- [Oracle ILOM Features and Functionality](#)
- [Supported Management Interfaces](#)
- [Supported Operating System Web Browsers](#)
- [Integration With Other Management Tools](#)

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 2-1 Oracle ILOM Features and Functionality

Oracle ILOM Feature	What You Can Do
Newly designed web and command-line interfaces	Display high-level information in a simple, standardized format that is common across x86 and SPARC SP platforms.
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"> • Oracle ILOM automatically learns the network address of the server SP using IPv4 and IPv6 default settings. • Configure BIOS settings on the x86 SP platform.
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 health and system event logs. • Monitor hardware event logs. • Monitor audit event logs. • Monitor customer-replaceable units (CRUs) and field-replaceable units (FRUs), including power supplies, fans, host bus adapters (HBAs), PCI devices, disks, CPUs, memory, and the motherboard. • Monitor environmental temperatures (component temperatures).
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 through the serial port and LAN. • Access the 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, or floppy to the system for remote storage.
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 immediate shutdown or perform a graceful shutdown to shut down the host operating system before power-off. • Monitor power management and power history charts through the web interface.
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"> • Log events in a consistent way for all “service” data. • Monitor hardware and system-related errors, as well as ECC memory errors reported on a dedicated user interface page and into SP logs, syslog, and remote log hosts. • Oracle ILOM automatically clears most fault conditions after you perform a service action to address the fault.
System alerts, including SNMP traps, IPMI PETs, remote syslog, and email alerts	<ul style="list-style-type: none"> • Monitor components using industry-standard SNMP commands and the IPMItool utility.

Supported Management Interfaces

This documentation provides conceptual and procedural information about the Oracle ILOM web and command-line interfaces. However, to access all of the Oracle ILOM features and functions, you can choose to use any of, or a combination of, the following interfaces and protocols.

- **Web interface** – The web interface enables you to access the Oracle ILOM SP through a web browser. From the Oracle ILOM 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. 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.
- **Simple Network Management Protocol (SNMP) interface** – Oracle ILOM also provides an SNMP v3 interface for third-party applications such as HP OpenView and IBM Tivoli. Some of the MIBs supported by Oracle ILOM include:
 - SUN-PLATFORM-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)

Related Information

- [Log In to the Oracle ILOM Web Interface](#)
- [Log In to the Oracle ILOM CLI](#)
- Server Management Using IPMI
- SNMP Overview
- Setting Up a Management Connection to Oracle ILOM and Logging In

Supported Operating System Web Browsers

Oracle ILOM supports the following operating system web browsers.



Note:

For a list of operating systems supported by the Oracle server, refer to the server administration guide or product release notes.

Table 2-2 Supported Web Browsers

Operating System	Web Browser
Oracle Solaris 10 and 11	<ul style="list-style-type: none"> • Mozilla Firefox ESR 45.2
Oracle Linux 7, Red Hat Enterprise Linux 7, SuSE Linux Enterprise 12, Ubuntu Linux LTS 14	<ul style="list-style-type: none"> • Mozilla Firefox 38.1 and 45.3
Microsoft Windows 7	<ul style="list-style-type: none"> • Google Chrome 55.02987 • Internet Explorer 11.04.41, 11.0.900 • Mozilla Firefox ESR 45.9
Microsoft Windows 10	<ul style="list-style-type: none"> • Google Chrome 57 • Internet Explorer 11 • Mozilla Firefox ESR 45.8
Apple Mac OS X 10.7 through 10.11 ^{1 2}	<ul style="list-style-type: none"> • Safari 10

¹ The storage redirection feature in the Oracle ILOM Remote System Console is not supported by Macintosh browser clients. In addition, international keyboard support is not supported by Macintosh browser clients.

² The Oracle ILOM Remote System Console Plus is not supported on Macintosh browser clients.

Related Information

- [Oracle ILOM Web Interface](#)
- [Log In to the Oracle ILOM Web Interface](#)

Integration With Other Management Tools

You can easily integrate Oracle ILOM with other management tools and processes. For links to documentation for supported third-party system management tools, go to:

<http://www.oracle.com/technetwork/documentation/sys-mgmt-networking-190072.html#thirdparty>

For information about the Oracle Enterprise Manager Ops Center management tool, see [About Oracle Enterprise Manager Ops Center](#).

About Oracle Enterprise Manager Ops Center

Oracle Enterprise Manager Ops Center can help you manage new and existing Oracle systems on your network. For instance, you can use Oracle Enterprise Manager Ops Center to:

- Update the server to the latest firmware and BIOS image.
- Provision the operating environment with off-the-shelf distributions or Oracle Solaris images.
- Manage updates and configuration changes.

- Remotely control key aspects of the service processor such as boot control, power status, and indicator lights.

For more information about Oracle Enterprise Manager Ops Center, go to: http://docs.oracle.com/cd/E27363_01/index.htm

3

Getting Started With Oracle ILOM

Description	Links
Log in to the Oracle ILOM CLI and web interface.	<ul style="list-style-type: none">• Logging In to Oracle ILOM
Learn about Oracle ILOM web interface navigation options .	<ul style="list-style-type: none">• Navigating the Web Interface
Learn about the Oracle ILOM CLI namespace and issuing CLI commands.	<ul style="list-style-type: none">• Navigating the Command-Line Interface (CLI) Namespace Targets

Related Information

- [Setting Up a Management Connection to Oracle ILOM and Logging In](#)
- [Server Management Using IPMI](#)
- [SNMP Overview](#)

Logging In to Oracle ILOM

- [Network Requirements for Logging In](#)
- [Log In to the Oracle ILOM Web Interface](#)
- [Log In to the Oracle ILOM CLI](#)

Network Requirements for Logging In

Before logging in to Oracle ILOM over a network connection, you must:

- Establish a physical network management connection to the server SP from either an internal trusted network or a secure private network.
- Obtain the network address assigned to the server SP.
The accepted input formats for entering IPv4 and IPv6 addresses are as follows:

 **Note:**

When entering an IPv6 address or Link-Local IPv6 address, the address must be enclosed within brackets to work correctly. However, when you specify an IPv6 address to log in to Oracle ILOM using SSH, *do not* enclose the IPv6 address in brackets.

- **IPv4 address** – 192.0.2.0
- **IPv6 address** – [2001:db8:0:0:0:0:0:0/32]
- **IPv6 address using SSH and root user account** – `ssh root@[ipv6address]`
- **Link-Local IPv6 address** – [e80::214:4fff:feca:5f7e/64]

- **DNS host domain address** – `company.com`
- If you do not have an Oracle ILOM user account, you will need to obtain a user account from your Oracle ILOM system administrator.

Related Information

- [Supported Operating System Web Browsers](#)
- [Log In to the Oracle ILOM Web Interface](#)
- [Log In to the Oracle ILOM CLI](#)
- [Setting Up a Management Connection to Oracle ILOM and Logging In](#)
- [Setting Up and Maintaining User Accounts](#)

Log In to the Oracle ILOM Web Interface

Before You Begin

Meet the requirements described in [Network Requirements for Logging In](#).

1. In the address bar of a web browser, type the IPv4 address, IPv6 address, or hostname of the server service processor (SP), and then press Enter.

The Oracle ILOM Login page appears.

2. Type a user name and password, and then click Log In.

Note:

To enable first-time login and access to Oracle ILOM, a default Administrator account and its password are provided with the system. To build a secure environment, you must change the default password (`changeme`) for the default Administrator account (`root`) after your initial login to Oracle ILOM. If this default Administrator account has since been changed, contact your system administrator for an Oracle ILOM user account.

Related Information

- [Supported Operating System Web Browsers](#)
- [Network Connection Issues: Oracle ILOM Interfaces](#)
- [Setting Up a Management Connection to Oracle ILOM and Logging In](#)
- [Default Timeout for CLI and Web Sessions](#)
- [Password Recovery for Default root Account](#)

Log In to the Oracle ILOM CLI

Before You Begin

Meet the requirements described in [Network Requirements for Logging In](#).

1. Using a Secure Shell (SSH) session, log in to Oracle ILOM in one of the following ways:

- If you are logging in with the default `root` account password, type the following at the system prompt:

```
$ ssh root@ system-ip-address
```

 **Note:**

To enable first-time login and access to Oracle ILOM, a default Administrator account and its password are provided with the system. To build a secure environment, you must change the default password (`changeme`) for the default Administrator account (`root`) after your initial login to Oracle ILOM. If this default Administrator account has since been changed, contact your system administrator for an Oracle ILOM user account.

- If you are logging in with a user account that was created for you by the system administrator, type the following at the system prompt:

```
$ ssh system-ip-address
```

If Oracle ILOM is operating in a dual-stack network environment, you can enter the `system-ip-address` in either an IPv4 or IPv6 address format.

2. At the system prompt, type the password of your user account. (For the default root account, this is `changeme`.)

The Oracle ILOM CLI prompt appears (->).

For example:

```
Password: password
```

```
Oracle(R) Integrated Lights Out Manager
```

```
Version 3.2.1.0 r76641
```

```
Copyright (c) 2012, Oracle and/or its affiliates. All rights reserved.
```

```
->
```

Related Information

- [Network Connection Issues: Oracle ILOM Interfaces](#)
- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Setting Up a Management Connection to Oracle ILOM and Logging In](#)
- [Password Recovery for Default root Account](#)

Navigating the Web Interface

- [Oracle ILOM Web Interface](#)
- [Web Interface Navigation Options](#)
- [Chassis View for SPARC M8 and M7 Series Systems](#)

Oracle ILOM Web Interface

Oracle ILOM Web Interface Summary Information Page

The screenshot displays the Oracle ILOM Web Interface Summary Information page. The interface includes a navigation pane on the left, a main content area with a 'Summary Information' section, and a 'Status' section at the bottom. Numbered callouts (1-11) identify key UI elements: 1 points to the navigation pane; 2 points to a warning message icon; 3 points to the user field; 4 points to the role field; 5 points to the hostname field; 6 points to the 'About' button; 7 points to the 'Refresh' button; 8 points to the 'Logout' button; 9 points to the 'General Information' table; 10 points to the 'Actions' panel; and 11 points to the 'Status' table.

Number	Description
1	Navigation pane – A hierarchical menu that enables you to navigate through the web interface.
2	Warning message – Displays the number of warnings that Oracle ILOM detected on the managed server SP. You can define warning thresholds and define when and where you receive alerts from the ILOM Administration > Notifications page. For more information, refer to <i>Configuring Alert Notifications, Service Requests, or Remote Logging in Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 5.0.x</i> .
3	User field – Displays the user name of the Oracle ILOM account that was used to log in.
4	Role field – Displays the role privileges assigned to the user account that was used to log in.
5	Hostname field – Displays the hostname of the SP.
6	About button – Click to view product copyright information.
7	Refresh button – Click to refresh the information in the content pane of the interface. The Refresh button does not save new data that you might have entered or selected on the page.

Number	Description
8	Log Out button – Click to end the current session of the web interface.
9	General Information panel – Displays information about the server, such as the system type, serial number, installed firmware version, and service processor IP address.
10	Actions panel – Enables you to perform common server management actions, such as powering the system on or off, and launching the remote console application.
11	Status panel – Provides an overview of each server subsystem, including a health status and component count.

Web Interface Navigation Options

The following table describes the web interface navigation options available for devices managed by Oracle ILOM.



Note:

The server SP navigation options presented in the web interface might differ slightly depending on the Oracle ILOM firmware version currently installed on the managed device.

Table 3-1 Managed Server SP - Web Interface Navigation Options

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
System Information	Summary	View summary information about the system. You can also perform the following actions: <ul style="list-style-type: none"> • Turn the system power state on or off. • Locate the system in the chassis by turning on or turning off the system indicator LED. • Update the system firmware. • Launch the Remote Console. • View the overall system status and problem count. 	Server SP Domain
	Processors	View summary and detailed information about the processors in the system.	Server SP
	Memory	View summary and detailed information about the memory installed in the system.	Server SP

Table 3-1 (Cont.) Managed Server SP - Web Interface Navigation Options

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
	Power	View summary and detailed information about the power supplies in the system.	Server SP
	Cooling	View summary and detailed information about the fans that cool the system.	Server SP
	Storage	View summary information about the storage in the SP. Oracle ILOM reports on the following storage: <ul style="list-style-type: none"> • Disks • Volumes (including logical volumes) • Controllers • Expanders 	Server SP
	Networking	View summary and detailed information about system networking.	Server SP
	PCI Devices	View summary and detailed information about the PCI devices in the system.	Server SP
	Firmware	View the current firmware levels and choose to upgrade the firmware, if needed.	Server SP
Open Problems		View information about systems and subsystems that are in a faulted state.	Server SP
Remote Control	Redirection	Manage the host remotely by redirecting the system console to your local machine.	Server SP Domain
	KVMS	Enable or disable remote management of keyboard, video, mouse, or storage devices.	Server SP Domain
Host Management	Power Control	Select a power state: Immediate Power Off, Graceful Shutdown and Power Off, Power On, Power Cycle, or Reset.	Server SP Domain
	Diagnostics	Enable or disable diagnostics for x86 processor-based systems or SPARC processor-based systems.	Server SP Domain
	Host Control	View and configure the host control information. Configure the boot device at the next system power-on.	Server SP Domain
	Host Boot Mode	Override the default server boot method on a SPARC server.	Server SP Domain
	Host Domain	Configure host domain control settings and view the host domain configurations on a SPARC server.	Server SP Domain

Table 3-1 (Cont.) Managed Server SP - Web Interface Navigation Options

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
	Keyswitch	Control the position of the virtual keyswitch on a SPARC server.	Server SP Domain
	TPM	Manage the state of the Trusted Platform Module feature on a SPARC server.	Server SP Domain
System Management	BIOS	Manage the BIOS configuration backup and restore.	Server SP
	Domains	View and manage the Domain Configurable Unite (DCU) availability and assignments for hosts on a SPARC multi-domain server.	Server SP
	Policy	Enable or disable system power policies.	Server SP
	Diagnostics	Select triggers that will cause a Power On Self Test to be run on the single server SP or a SPARC multi-domain server.	Server SP
Power Management	Consumption	View power consumption metrics for actual power and permitted power, as well as set power consumption thresholds to generate email alerts or SNMP notifications.	Server SP Domain
	Limit	View or configure server power limits.	Server SP Domain
	Allocation	View system power requirements for capacity planning.	Server SP Domain
	Settings	Configure policy options for power consumption on SPARC servers.	Server SP Domain
	Redundancy	View and configure power supply redundancy options.	Domain
	Statistics	View power statistical data for Oracle server SP or SPARC multi-domain server.	Server SP Domain
	History	View a history of rolling averages for power consumption.	Server SP Domain
ILOM Administration	Identification	Enter or change the service processor identification information by assigning a host name or system identifier.	Server SP
	Logs > Event	View various details about each event, including the event ID, class, type, severity, date and time, and description of the event.	Server SP
	Logs > Audit	View interface-related user actions such as user logins, logouts, configuration changes, and so on.	Server SP

Table 3-1 (Cont.) Managed Server SP - Web Interface Navigation Options

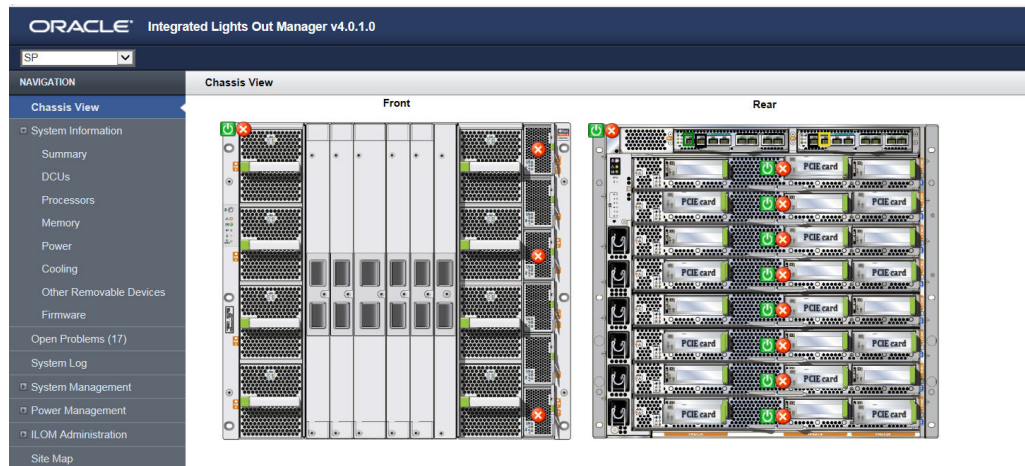
First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
	Management Access > Web Server	Edit or update the web server settings, such as the HTTP web server or the HTTP port.	Server SP
	Management Access > SSL Certificate	View information about the default SSL certificate, or optionally upload a new SSL certificate.	Server SP
	Management Access > SNMP	View SNMP settings.	Server SP
	Management Access > SSH Server	Configure Secure Shell (SSH) server access and private key generation.	Server SP
	Management Access > IPMI	Use a command-line interface to monitor and control your server platform, as well as to retrieve information about your server platform.	Server SP
	Management Access > CLI	Configure the CLI settings. The Session Time-out value indicates the number of idle minutes that can lapse before automatic CLI logout occurs.	Server SP
	Management Access > Banner Messages	View and configure the message that appears prior to user login and the message that appears after user login.	Server SP
	User Management > Active Sessions	View the users who are currently logged in to Oracle ILOM, as well as the type of session initiated.	Server SP
	User Management > User Accounts	Add, delete, or modify local Oracle ILOM user accounts.	Server SP
	User Management > LDAP	Configure Oracle ILOM access for LDAP users.	Server SP
	User Management > LDAP/SSL	Configure Oracle ILOM access for LDAP users with enhanced security settings enabled by Secure Socket Layer (SSL) technology.	Server SP
	User Management > RADIUS	Configure Oracle ILOM access for RADIUS users.	Server SP
	User Management > Active Directory	Configure Oracle ILOM access for Active Directory users.	Server SP
	Connectivity > Network	View and edit the IPv4 and IPv6 network settings for Oracle ILOM and for local interconnect interface settings.	Server SP
	Connectivity > DNS	Specify host names, and have those host names resolved into IP addresses using the Domain Name Service (DNS).	Server SP
	Connectivity > Serial Port	View and edit the baud rate of the internal and external serial ports.	Server SP

Table 3-1 (Cont.) Managed Server SP - Web Interface Navigation Options

First-Level Menu	Second- and Third-Level Menu	What You Can Do	Managed Device
	Configuration Management > Backup/Restore	Back up and restore the service processor configuration to a remote host or removable storage device in a secure manner.	Server SP
	Configuration Management > Reset Defaults	Restore all Oracle ILOM default settings.	Server SP
	Notifications > Alerts	View details about each alert, and change the list of configured alerts.	Server SP
	Notifications > Syslog	Configure the server addresses to which the syslog messages will be sent.	Server SP
	Notifications > SMTP Client	Configure the state of the SMTP client, which is used for sending email notifications of alerts.	Server SP
	Date and Time > Clock	View and edit the Oracle ILOM clock time manually, or synchronize the Oracle ILOM clock with an NTP server.	Server SP
	Date and Time > Timezone	Specify a particular time zone so that time stamps displayed by the service processor can be correlated to logs created elsewhere (for example, in the Oracle Solaris operating system).	Server SP
	Maintenance > Firmware Upgrade	Start the process of updating the Oracle ILOM firmware.	Server SP
	Maintenance > Reset Components	Reset the service processor.	Server SP
	Maintenance > Snapshot	Collect environmental, log, error, and FRUID data and send it to a USB flash drive, or an external host using the CLI, or as a downloaded file.	Server SP

Chassis View for SPARC M8 and M7 Series Systems

Use the Oracle ILOM Chassis View page on M8 and M7 SPARC systems to view the overall health of the chassis components. This interactive page provides a pictorial representation of the system chassis health state. The colored indicators on the page indicate the individual component health state. For example, a red X indicates a faulted hardware state, a yellow exclamation point is a warning to indicate a service action is required, and a green checkmark indicates that the component health is OK and no service action is required. Hovering over or clicking on an individual chassis component provides further details and health state.



For further details on component health states and resolution information for faulted or service required components, see:

- [Viewing System Inventory, Health, and Performing Service and Management Actions](#)
- "View Status and Faults in Chassis View (Oracle ILOM)" in the *Oracle SPARC M8 and SPARC M7 Servers Administration Guide*
- "View Status and Faults in Chassis View (Oracle ILOM)" in the *Oracle SPARC M8 Service Manual*

Navigating the Command-Line Interface (CLI) Namespace Targets

- [Oracle ILOM CLI Supports Case Insensitive Expressions](#)
- [Oracle ILOM CLI Namespace Targets](#)
- [Managing PDomains From a SPARC Multi-Domain Server](#)
- [Navigating Target Properties and Viewing Supported Commands](#)

Oracle ILOM CLI Supports Case Insensitive Expressions

The Oracle ILOM command-line interface (CLI) is case insensitive, that is, Oracle ILOM does not distinguish between uppercase and lowercase characters. The following are exceptions to this rule:

- Targets and properties under the `/SYS` legacy target for server service processors (SPs)
- Command verbs, such as `show`, `set`, and `start`
- Property values

Oracle ILOM CLI Namespace Targets

The Oracle ILOM CLI namespace is a hierarchical tree that contains every manageable object on an Oracle server system.

The following table describes the CLI namespace targets . The namespace targets listed in the following table are at the highest level in the tree hierarchy.

Managed Device(s)	Namespace Target	Namespace Description
Server SP	/SP	On a server SP, the properties under /SP namespace are used for 1) configuring the Oracle ILOM service processor (SP), 2) viewing log entries, 3) managing sub-components, and 4) accessing remote consoles.
	/HOST	On a server SP, the properties under the /HOST namespace target are used to monitor and manage the host operating system that is installed on a rackmount server or blade server module.
Server SP	/System	On a server SP, the properties under the /System namespace are used to monitor the hardware health and system inventory, as well as to perform maintenance actions such as firmware updates. The names under the /System namespace directly correspond to the hardware components installed on the managed device.
SPARC Multi-Domain Server SP	/Servers	On a SPARC multi-domain server SP, the properties under the /Servers namespace are used to monitor and manage the hardware sub-component configurations. For example, from a SPARC multi-domain server SP, you can manage PDomains configurations (/Servers/PDomains)
Server SP	/SYS	On a server SP, the /SYS namespace is a pre-Oracle ILOM 3.1 legacy target. It is only visible when the property for legacy_targets is enabled on the managed device. On rackmount or blade servers, this target type is similar to the /System target, but includes all targets available for Oracle ILOM 3.0. The targets and properties under /SYS namespace are always available (whether you see them or not) to ensure backward compatibility with existing Oracle ILOM user scripts.

Managed Device(s)	Namespace Target	Namespace Description
	/STORAGE (3.0 legacy target)	On a server SP, the /Storage namespace is a pre-Oracle ILOM 3.1 legacy target. It is only visible when property for legacy_targets is enabled on the managed device. This target was previously used to manage storage components, such as SAS storage devices. The /Storage namespace target and properties are always available (whether they are visible or hidden) to ensure backward compatibility with existing Oracle ILOM user scripts.

Related Information

- [CLI Hierarchy for Oracle ILOM 5.0.x Targets](#)

CLI Hierarchy for Oracle ILOM 5.0.x Targets

Here is an example of the namespace hierarchy for a server that ships with Oracle ILOM firmware versions 5.0 or later. Legacy targets are hidden by default.

Table 3-2 Example Oracle ILOM 5.0.x CLI Targets

Server SP CLI Namespace Example
/HOST <ul style="list-style-type: none"> • bootmode (SPARC only) • console • diag • domain (SPARC only) • provisioning (x86 only) • tpm (SPARC only)
/System <ul style="list-style-type: none"> • Cooling • Processors • Memory • Power • Storage • PCI_Devices • Firmware • Networking • Open_Problems • BIOS (x86 only) • IO_Modules

Table 3-2 (Cont.) Example Oracle ILOM 5.0.x CLI Targets

Server SP CLI Namespace Example
/SP
<ul style="list-style-type: none">• alertmgmt• cli• clients• clock• config• diag• faultmgmt• firmware• logs• network• policy• powermgmt• preferences• serial• services• sessions• users

Related Information

- [CLI Device Management Namespace Summary](#)
- [CLI Reference for Mapping Management Tasks to CLI Targets](#)
- [Managing PDomains From a SPARC Multi-Domain Server](#)

Managing PDomains From a SPARC Multi-Domain Server

You can manage PDomains directly from a SPARC multi-domain server SP CLI session. To view and manage the PDomain properties from a multi-domain server SP CLI session, append `/Servers/PDomains/PDomain_n` to the `/SP` target.

Related Information

- [CLI Device Management Namespace Summary](#)
- [CLI Reference for Mapping Management Tasks to CLI Targets](#)

Navigating Target Properties and Viewing Supported Commands

Use the following commands to navigate the Oracle ILOM command-line interface (CLI) namespace:

- `help targets` – List all available targets in the CLI namespace for your system with a brief description.
- `cd` – Navigate the namespace hierarchy.

For example, to navigate to the `services` target under `/SP`, type:

cd /SP/services

- `show` (or `ls`) – List the targets immediately under a higher-level target and the commands that can be used with that target.

For example, to list information about the `/SP/services` target, type:

```
-> cd /SP/services
/SP/services
-> show
/SP/services
  Targets:
    http
    https
    ipmi
    kvms
    servicetag
    snmp
    ssh
    sso

  Properties:

  Commands:
    cd
    show
```

 **Note:**

You can issue commands from anywhere in the CLI hierarchy as long as you use a fully qualified path and the command is supported by the intended target. In the previous example, you could have entered **`show /SP/services`** to yield the same result.

In the previous example, the `show` command output showed properties and commands in a simple list; however, the `show` command might display properties and commands in a tabular output. For example:

```
-> show -o table SP/services/http
Target          | Property          | Value
-----+-----+-----
/SP/services/http | port              | 80
/SP/services/http | securereredirect  | enabled
/SP/services/http | servicestate      | disabled
/SP/services/http | sessiontimeout    | 15

->
```

- `help` – Display properties, possible property values, and role requirements for setting configurable properties for a given target.

 **Note:**

Not all targets have configurable properties. Some are read only.

For example, to obtain help information about the `http` target, which is used to configure the Oracle ILOM internal web server for HTTP access, type:

```
-> help /SP/services/http
```

```
/SP/services/http : HTTP service
```

```
Targets:
```

```
Properties:
```

```
port : Port number for http service
```

```
port : User role required for set = a
```

```
secureredirect : HTTP secure redirect
```

```
secureredirect : Possible values = enabled, disabled
```

```
secureredirect : User role required for set = a
```

```
servicestate : HTTP service state
```

```
servicestate : Possible values = enabled, disabled
```

```
servicestate : User role required for set = a
```

```
sessiontimeout : Timeout in minutes for http session
```

```
sessiontimeout : Possible values = Range: 1-720 minutes
```

```
sessiontimeout : User role required for set = a
```

```
->
```

Related Information

- [Oracle ILOM CLI Namespace Targets](#)
- [Using the Command-Line Interface](#)

4

Viewing System Inventory, Health, and Performing Service and Management Actions

Description	Links
Gather system information and view subcomponent health details.	<ul style="list-style-type: none">Viewing System Component Inventory and Health Status
View open problems and determine required service actions.	<ul style="list-style-type: none">Administering Open Problems
Perform service actions for M-Series servers removable devices.	<ul style="list-style-type: none">Administering Removable Devices on SPARC M-Series Servers
Access and manage logging entries for system events and user actions.	<ul style="list-style-type: none">Managing Oracle ILOM Log Entries
Perform common system management actions from the web interface.	<ul style="list-style-type: none">Performing Common System Management Actions

Related Information

- [Configuring Host Server Management Actions](#)
- [Setting System Management Power Source Policies and Device Monitoring](#)
- [Configuring Alert Notifications, Service Requests, or Remote Logging](#)

Viewing System Component Inventory and Health Status

The Oracle ILOM interfaces provide easy-to-access properties for viewing server component inventory and health status. For further details, see

- [View System-Level Information and Health Status \(Web\)](#)
- [View Subcomponent-Level Information and Health Status \(Web\)](#)
- [View System-Level Identification and Health Status \(CLI\)](#)
- [View Subcomponent-Level Information and Health Status \(CLI\)](#)
- [Health State: Definitions](#)

View System-Level Information and Health Status (Web)

The system-level health status properties for a host server are viewable from the Summary page in the web interface.

1. To view system-level health status details, click System Information > Summary.
The Summary page appears.
2. To collect system information about the managed device, review the entries in the General Information table.

Information in the General Information table can include the model number, serial number, system type, firmware currently installed, primary operating system installed, host MAC address, IP address and MAC address for the managed SP.

 **Note:**

The property value for the Primary Operating System installed is shown only when the Oracle ILOM Hardware Management Pack is installed on the managed device.

3. To identify problems detected on the managed device or to view the total problem count, review the entries in the Status table.

The overall health status and total problem count appear at the top of the table.

To view additional information about a subcomponent category reported in the Status table, click the link in the Subsystem column.

4. To view the firmware history on the managed device, click System Information > Firmware.

Related Information

- [Health State: Definitions](#)
- [View Subcomponent-Level Information and Health Status \(Web\)](#)
- [Administering Open Problems](#)

View Subcomponent-Level Information and Health Status (Web)

The subcomponent-level health status properties for a host server are viewable from the Summary page in the web interface.

Before You Begin

- To view health and inventory status properties on the Networking page for Infiniband network controllers, the installation of the Oracle Hardware Management Pack (HMP) software, version 2.3 or later, is required.
- To view the majority of the health and inventory status properties on the Storage page, the installation of the HMP software, version 2.2 or later, is required. In addition, to view the controller **Type** property or the controller **Details** properties (such as, Location; World Wide Name (WWN) for FC Controllers; and, Number Of Ports), the installation of HMP software, version 2.3 or later, is required.

1. To view subcomponent-level health status properties, click System Information > subcomponent-category-name.

For example:

- An SP navigation pane shows a list of subcomponents such as Processors, Memory, Power, Cooling, Storage, and so on.
To view server SP subcomponent-level health status details for Processors, click System Information > Processors.
- A Domain navigation pane shows subcomponents such as DCUs, Processors, Memory, Power, Cooling, Storage, Networking, PCI Devices, and Firmware.
To view subcomponent-level health status details for domain-specific DCUs, click System Information > DCUs.

 **Note:**

Domain navigation panes are available for Oracle's multi-domain SPARC systems.

2. On the subcomponent category page, you can:
 - Determine the overall health for the subcomponent category and the number of subcomponents installed for each category.
 - Determine the health details and the installed location for each subcomponent currently installed on the managed device.

On some servers, you can also enable and disable subcomponents from the subcomponent category page. For further information about enabling or disabling subcomponents on your Oracle server, refer to the documentation supplied with the server.

- View further information about the installed subcomponent by clicking the Details link in the table.

 **Note:**

In the DIMM Details page, as of Oracle ILOM 3.1.2, the following format will be used to describe the value for the DIMM Part Number = *Oracle_part number, vendor_part_number*. For example:
5111616-01, M393B5270DH0-YK0; *where*: 5111616-01 is the Oracle part number and M393B5270DH0-YK0 is the vendor part number.

Related Information

- [Health State: Definitions](#)
- [Administering Open Problems](#)

View System-Level Identification and Health Status (CLI)

The system-level identification and health status CLI properties are viewable at the `/System` target.

- To collect system-level information or to verify the system health status, type:

```
show /System
```

For example:

Properties:

```
health = Service Required
health_details = PS1 (Power Supply 1) is faulty. Type 'show
/System/Open_Problems' for details.
open_problems_count = 1
type = Rack Mount
model = ORACLE SERVER X5-2L
qpart_id = Q10543
part_number = X5-2L-P1.LAST-20
serial_number = 1435NM702B
component_model = ORACLE SERVER X5-2L
component_part_number = X5-2L-P1.LAST-20
```

```

component_serial_number =
000000000011111111222222223333333344444444
                                44455555555556666
system_identifier = (none)
system_fw_version = 5.0.0.0
primary_operating_system = Not Available
primary_operating_system_detail = Comprehensive System monitoring is
                                not available. Ensure the host is
                                running with the Hardware

Management
                                Pack. For details go to
                                http://www.oracle.com/goto/ilom-

redire
                                ct/hmp-osa
host_primary_mac_address = 00:10:e0:62:71:30
ilom_address = 10.153.55.47
ilom_mac_address = 00:10:E0:62:71:34
locator_indicator = Off
power_state = Off
actual_power_consumption = 21 watts
action = (Cannot show property)

```

 **Note:**

As of Oracle ILOM 4.0.4, the permissible length of the system-level serial number identifiers for System, Product and Chassis were increased to 64 characters. The default host name is formed by concatenating an Oracle branding string, such as "ORACLESP-", with the system-level serial number. If the length of the system serial number is greater than 50 characters, the default host name is truncated since it has a length of 60 characters, missing the characters after the 50th character in the serial number. In this case, the system administrator should overwrite the default host name with a customer defined hostname. For further information on how to overwrite the default hostname, see Assigning System Identification Information.

 **Note:**

The property value for the primary operating system installed on the managed device is shown only when the Oracle ILOM Hardware Management Pack is installed on the managed device.

Related Information

- [Health State: Definitions](#)
- [View Subcomponent-Level Information and Health Status \(CLI\)](#)
- [Administering Open Problems](#)

View Subcomponent-Level Information and Health Status (CLI)

The host health status CLI properties for sub-components are viewable under the / System target.

- To access subcomponent-level health details from the CLI, type:

```
show /System / [subcomponent-category-name]
```

Where [subcomponent-category-name] equals one of the subcomponent target names under show /System.

 **Note:**

For Oracle's multi-domain SPARC systems, use the following CLI path to view subcomponent-level health details for a PDomain: /Servers/PDomains/PDomain_n/System/subcomponent-category-name

For example:

- To view the subcomponent health status for memory modules on a single server SP system, type:

```
show /System/Memory
```

```
/System/Memory
Targets:
  DIMMs

Properties:
  health = OK
  health_details = -
  installed_memory = 16 GB
  installed_dimms = 2
  max_dimms = 16

Commands:
  cd
  show
```

- To view the subcomponent health status for a specific DIMM on a single server SP, type:

```
show /System/Memory/DIMMs/DIMM_n
```

```
/System/Memory/DIMMs/DIMM_0  Targets:  Properties:  health =
OK      health_details = -      part_number = 001-0003
serial_number = 00AD0111232F6E432B      location = P0/D0 (CPU 0 DIMM
0)      manufacturer = Hynix Semiconductor Inc.      memory_size = 8 GB
Commands:      cd      show
```

 **Note:**

In the DIMM_n properties, as of Oracle ILOM 3.1.2, the following format will be used to describe the value for the part_number = *Oracle_part number, vendor_part number*. For example: 5111616-01, M393B5270DH0-YK0; where: 5111616-01 is the Oracle part number and M393B5270DH0-YK0 is the vendor part number.

Related Information

- [Health State: Definitions](#)
- [Administering Open Problems](#)

Health State: Definitions

Health Status State	Description
Not Available	Oracle ILOM is unable to provide a health status for this component. Oracle ILOM might require the Hardware Management Pack to be installed. For more information, see the Oracle Hardware Management documentation library at: http://www.oracle.com/pls/topic/lookup?ctx=ohmp&id=homepage
OK	The system or component is in good working order.
Offline	Offline applies to the Prepare to Remove action state of a chassis subcomponent. This status appears when the action property is set to Prepare to Remove and the physical subcomponent is not physically removed from the chassis. Note: Not all server chassis subcomponents managed by Oracle ILOM support properties for service actions (Prepare to Remove or Return to Service).
Warning	Oracle ILOM presents informational warning messages to indicate that a minor problem has been detected on a managed device. Despite any warning messages, the managed device is functioning as expected and the informational message can be safely ignored.
Degraded	Oracle ILOM indicates a Degraded state for a parent component if one or more of its subcomponents are disabled. The parent component continues to participate in the operation of the system in a limited capacity.
Disabled	Oracle ILOM presents a Disabled state when one of the following conditions occurs: <ul style="list-style-type: none"> • A fault was not detected on the component, however, Oracle ILOM has determined that the component should not participate in the operation of the system. • An end-user has manually disabled the component. If a Disabled health state appears, view the Health Details property for the component.
Disabled (Service Required)	Oracle ILOM has detected a fault on the component and disabled it. A service action is required to enable the disabled component. If a Disabled (Service Required) health state appears, view the Health Details property provided for the component.
Service Required	Oracle ILOM has detected a problem on the managed device that will require a service action to resolve the issue. If this status appears at the system level, view the open problems detected on the managed device in the Oracle ILOM web interface or CLI. If this status appears in the Open Problems table, refer to the URL provided in the table for further details.

Related Information

- [Administering Open Problems](#)

Administering Open Problems

Oracle ILOM automatically detects system hardware faults and environmental conditions on a managed device. If a problem occurs on a managed system, Oracle ILOM automatically:

- Illuminates the Server Action LED on the physical device.
- Identifies the faulted condition in an easy-to-read Open Problems table.
- Records system information about the fault condition in the event log.

Upon the repair (or the replacement) of a faulty server component, Oracle ILOM automatically clears the fault state from the Open Problems table.

For further information about administering open problems that are detected and reported in Oracle ILOM interfaces, see these topics:

- [Open Problems Terminology](#)
- [View Open Problems Detected on a Managed Device](#)

Open Problems Terminology

Term	Definition
Faulted state	A <i>faulted state</i> indicates the component is present but is unusable or degraded because one or more problems have been diagnosed by Oracle ILOM. Oracle ILOM automatically disables the component to prevent damage to the system.
Open Problems	<i>Open Problems</i> refers to the Open Problems page in the web interface or the Open Problems tabular output shown in the CLI. When a problem is detected on a managed device, Oracle ILOM identifies the problem in the Open Problems CLI output or web interface table.
Oracle ILOM Fault Management Shell	The <i>Oracle ILOM Fault Management Shell</i> enables Oracle Services personnel to diagnose system problems and, if necessary, to override fault states. Customers should not use this shell unless requested to do so by Oracle Services.

View Open Problems Detected on a Managed Device

Open problems detected on a host server are viewable from either the Open Problems web page or the `/System/Open_problems` CLI target.

Before You Begin

- Faults reported in the Open Problems table for server components are automatically cleared upon repair or replacement of the component.
- Faults reported in the Open Problems table for customer-replaceable units (CRUs) must be manually cleared from the Open Problems table after repair or replacement. For instructions, see [Clear Faults for Undetected Replaced or Repaired Hardware Components](#).

To view host server open problems using the CLI or web interface, follow this step:

1. Perform one of the following:
 - **Web:**
Click System Information > Open Problems.

- **CLI:**
Type: `show /System/Open_Problems`
2. The Open Problems web page and the CLI target report the following information:
 - The total number of problems detected
 - The time stamp, name, and CLI target for each faulted component
 - The URL for troubleshooting a faulted component

Related Information

- [Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell](#)
- [Updating Oracle ILOM Firmware](#)
- [Reset Power to Server SP](#)

Administering Removable Devices on SPARC M-Series Servers

As of firmware release 3.2.5, Oracle ILOM provides a set of properties to manage removable devices, as well as to view the health, location, and inventory of removable devices in an M-series server. For further details on how to administer removable devices on an M-series servers, see the following procedure

- [Manage M-Series Server Removable Devices](#)

Manage M-Series Server Removable Devices

Before You Begin

- The Reset and Host Control (r) role is required in Oracle ILOM to perform a Prepare to Remove or Return to Service action.
- To view specific information about the removable device properties appearing on the web page, click the More Details... link at the top of the page.
- To view specific information about the CLI removable device properties, issue the `help` command. For example: `help /System/Other_Removable_Devices/`



Note:

Not all components managed by Oracle ILOM support the Prepare to Remove and Return to Service service actions.

To administer the removable devices on an M-series server, following these steps:

1. To view the health and inventory of all removable devices on the server, perform one of the following:
 - Web (SP) Steps:
Click System Information > Other Removable Devices > Health.

View the Installed *[Device Name]* properties and the health information provided for all removable devices.

- CLI Steps:
 - a. To view a list of installed removable device names on the server, type:


```
show /System/Other_Removable_Devices
```
 - b. To view the inventory and health for a specific type of removable device, perform the following:
 - To view the inventory, type:


```
show /System/Other_Removable_Devices/  
[Installed_Device_Name]
```
 - To view the health, type:


```
show /System/Other_Removable_Devices/  
[Installed_Device_Name]/[Installed_Device_Name_n]
```
- 2. To remove a removable device for service or to return a removable device from service, perform one of the following:
 - Web (SP) Steps:
 - a. Click System Information > Other Removable Devices >[Name of Device].
 - b. In the table, select the component that needs to be removed or returned to service, for example Fan_Module 0.
 - c. At the top of the table, select one of the following service actions in the Actions list box:
 - Prepare to Remove
 - Return to Service
 A confirmation dialog box appears.
 - d. In the confirmation dialog box, click Yes to continue.
The health state for the removable device is updated to reflect your selection. For more information, see [Health State: Definitions](#).
 - CLI (SP) Steps:
 - a. Navigate to removable device that needs to be removed or returned to service. For example, to navigate to the Fan_Module 0 CLI target, you would type:


```
cd /System/Other_Removable_Devices/Fan_Modules/Fan_Module_0
```
 - b. Issue one of the following service actions:
 - To prepare device for removal, type:


```
set action=prepare_to_remove
```
 - To return device to service, type:


```
set action=return_to_service
```
 - c. At the prompt, type **Yes** to continue.
The health state for the component is updated to reflect the service action you set.
 - d. To verify the updated health state for the component, type:


```
show health
```



For more information about health states, see [Health State: Definitions](#).



Managing Oracle ILOM Log Entries

Oracle ILOM maintains four system management logs: system log, event log, audit log, and syslog. For further details about these logs, see the following topics:

- [Log Descriptions](#)
- [Log Properties](#)
- [Log Time Stamps](#)
- [View and Clear Log Entries \(Web\)](#)
- [View and Clear Log Entries \(CLI\)](#)
- [Filter Log Entries](#)

Log Descriptions

Log	Description
Audit	<p>The <i>audit log</i> tracks all interface-related user actions, such as user logins, user logouts, configuration changes, and password changes. The user interfaces monitored for user actions include the Oracle ILOM web interface, CLI, Fault Management Shell (captive shell), and Restricted shell, as well as SNMP and IPMI client interfaces.</p> <p>The audit log is helpful for auditing user activity to ensure that no privilege violations have occurred.</p>
	<div data-bbox="829 1079 1380 1346"><p> Note:</p><p>As of Oracle ILOM firmware version 5.1.0, user session login and logout events for all Oracle ILOM user interfaces (web, CLI, and API) have been moved from the audit log to the session log.</p></div> <div data-bbox="829 1381 1380 1591"><p> Note:</p><p>User login and logout events captured in the audit log prior to Oracle ILOM 5.1.0 will continue to remain in the audit log.</p></div>
Event	<p>The <i>event log</i> tracks informational, warning, or error messages about a managed device such as the addition or removal of a component or the failure of a component. The event properties recorded in the event log can include: the severity of the event, the event provider (class), and the date and time the event was logged.</p> <p>The event log is helpful for troubleshooting the system when problems occur. It is also helpful for monitoring the performance of the managed device.</p>

Log	Description
Session	<p>The <i>session log</i>, as of Oracle ILOM 5.1.0, tracks session IDs at the onset of a KVMS or a Serial Redirection user session.</p> <p>The session log is helpful to manage user access to KVMS and Serial Redirection connections, as well as differentiate between the different user sessions.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>The session log is only available in Oracle ILOM for KVMS or Serial Redirection connections opened on Oracle servers supporting Oracle ILOM 5.0 or later.</p> </div>
Syslog	<p>The <i>syslog</i> defines a set of common features for event logging and a protocol for transmitting the log entries to a remote host.</p> <p>The syslog is helpful if you want to combine events from multiple Oracle ILOM sessions in one place. The entries recorded in the syslog contain all the same information that you would see in the local event log.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>The syslog feature in Oracle ILOM is disabled by default. For instructions on how to configure the syslog properties in Oracle ILOM, refer to the Configuring Alert Notifications, Service Requests, or Remote Logging.</p> </div>
System	<p>The top-level <i>system log</i> presents a subset of relevant operational event log entries. Specifically, this log reports subsystem level diagnostic events pertaining to system inventory actions and component health. These events can include power on and off, FRU insertion and removal, as well as health status events, such as service required, warning, or OK.</p>

Log Properties

Property	Description	Applicable to:
Event ID	Unique number used to identify the encountered event.	<ul style="list-style-type: none"> • System Log • Event Log • Audit Log

Property	Description	Applicable to:
Date and Time	<p>Day and time the event occurred. If the Network Time Protocol (NTP) server is enabled to set the Oracle ILOM time, the Oracle ILOM clock uses Universal Coordinated Time (UTC).</p> <p>For more information about time stamps, see Log Time Stamps .</p>	<ul style="list-style-type: none"> • System Log • Event Log • Audit Log
Event Type or Type	<p>Hardware dependent event property.</p> <p>Event type examples:</p> <ul style="list-style-type: none"> • IPMI • UI • Upgrade • Persistence • Action or Service Required • Warning • OK 	<ul style="list-style-type: none"> • System Log • Event Log • Audit Log
Subsystem	<p>Hardware dependent property that identifies the subsystem where the event was encountered.</p> <p>Subsystem examples:</p> <ul style="list-style-type: none"> • System • Power • Cooling • Memory • Storage • I/O module • Processor • DCU • Firmware 	<ul style="list-style-type: none"> • System Log
Component	<p>Hardware dependent property that identifies the component where the event was encountered.</p> <p>Component examples:</p> <ul style="list-style-type: none"> • Host<i>n</i> • /System (Host System) • DCU<i>n</i> • PS<i>n</i> (Power Supply <i>n</i>) • Fan<i>n</i> (Fan <i>n</i>) • Disk<i>n</i> • ILOM 	<ul style="list-style-type: none"> • System Log

Property	Description	Applicable to:
Class	<p>Hardware dependent property that identifies the event class.</p> <p>Class examples:</p> <ul style="list-style-type: none"> • Audit/ Log – For commands that result in a configuration change. Description includes user, command, command parameters, and success/failure. • IPMI/Log – For any event that is recorded in the IPMI SEL is also put in the management log. • Chassis/State – For changes to the inventory and general system state. • Chassis/Action – For shutdown events for server, hot insert/removal of FRU components, as well as Reset Parameters button when pushed. • Fault/Fault – Description gives the time fault was detected and the suspect component name. • Fault/Repair – For Fault Management repairs. Description gives component name. 	<ul style="list-style-type: none"> • Event Log • Audit Log
Severity	<p>Severity level of the event.</p> <p>Severity examples:</p> <ul style="list-style-type: none"> • Debug • Down • Critical • Major • Minor 	<ul style="list-style-type: none"> • Event Log • Audit Log

Log Time Stamps

Local system time stamps, by default, are captured in the Oracle ILOM log files by using the host server system clock UTC/GMT time zone. However, if a log file is viewed from a remote client that is located in a different time zone, Oracle ILOM automatically adjusts the time stamps in the log files to reflect the local time zone of the remote client and the host system. In this case, two time stamps appear in the log for each listed event entry. In addition to supporting local system time stamps, Oracle ILOM enables you to capture remote router time stamps using a Network Time Protocol (NTP) server. For information about how Oracle ILOM captures time stamps for logged entries, refer to the Setting ILOM Clock Properties .

View and Clear Log Entries (Web)

Oracle ILOM log entries for a host server are viewable from the server SP web interface.

Before You Begin

- Admin (a) role privileges are required to clear log entries.

To view and clear log entries using the server SP web interface, follow these steps:

1. To view the log entries, perform one of the following:
 - To view the system log entries, click System Information > System Log.
 - To view the event or audit log entries, click ILOM Administration > Logs, and then click the Event or Audit tab.

The selected Oracle ILOM log page appears.

2. To clear all log entries shown, click the Clear Log button in the log table, and then click OK in the message box that appears.

Oracle ILOM removes all entries in log file.

Related Information

- [Filter Log Entries](#)
- [Configuring Syslog for Event Logging](#)
- [Setting ILOM Clock Properties](#)

View and Clear Log Entries (CLI)

Oracle ILOM log entries for a host server are viewable from the server SP CLI.

Before You Begin

- Admin (a) role privileges are required to clear log entries.

To view and clear log entries using the server SP CLI, follow these steps:

1. To view a tabular list of log entries, do one of the following:

- For the system log, type:
`show /System/Log/list`
- For the event log, type either:
`show /SP/Logs/event/list`
- For the audit log, type either:
`show /SP/Logs/audit/list`

To scroll through the list, press any key except the q key.

2. To clear log entries shown, type `set target clear=true` command, and then type `y` at the prompt.

To clear log entries shown, type `set target clear=true` command, and then type `y` at the prompt.

For example:

- `set /System/Log clear=true`
- `set /SP/logs/event/ clear=true`
- `set /SP/logs/audit clear=true`

Related Information

- [Filter Log Entries](#)
- [Configuring Syslog for Event Logging](#)
- [Setting ILOM Clock Properties](#)

Filter Log Entries

Properties for filtering the server SP log entries are available in the CLI and web interface.

 **Note:**

For a description of custom filters supported for each log type (Audit, Event, and System), see the online help in the web interface. To access the help, click the More Details ... link at the top of the web page. For example, click System Log then click the More details link located at the top of the web page.

To filter log entries for the server SP, follow these steps:

- To filter log entries, perform one of the following:
 - **From the web interface**, select either a standard filter or a custom filter from the Filter list box.

For further details about filtering log entries shown in the web interface, click the More Details link on the log page.

- **From the CLI**, issue the `show` command followed by one or more supported log filter properties.

For example:

- To filter the system log entries by Subcomponent or Event Type, type one of the following:

```
show /System/Log/list Subsystem== subsystem
```

```
show /System/Log/list Type== type
```

- To filter the event or audit log entries by Class, type:

```
show /SP/logs/ event|audit /list Class== class
```

- To filter the event or audit log entries by Class and Type, type:

```
show /SP/logs/ event|audit /list Class== class Type== type
```

- To filter the event or audit log entries using all the filter properties, type:

```
show /SP/logs/ event|audit /list Class== class Type== type  
Severity== value
```

Where:

- *subsystem* is the subsystem component name, for example: `System`, `Cooling`, or `Processor`. For other examples, see the Subsystem examples listed in the [Log Properties](#).
- *type* is the event name or the component name where the event occurred, for example: `OK`, `Warning`, `Service Required`, `Fann`, `Processorn`, `DCUn`, `DIMMn`, `UI`, `Product`, `Log`, `Update`, or `Action`. For other examples, see the Component or Event Type examples listed in the [Log Properties](#).
- *class* is the class event name, for example: `System`, `Fault`, `Chassis`, `Software`, `Audit`, `BIOS`, or `Sensor`. For further information about the Class log property, see Class in the [Log Properties](#).
- *severity* is the event severity, for example: `Debug`, `Down`, `Critical`, `Major`, or `Minor`.
- *event|audit* indicates a choice between the event and audit log. Type **event** to filter the event log, or type **audit** to filter the audit log.

Related Information

- [View and Clear Log Entries \(Web\)](#)
- [View and Clear Log Entries \(CLI\)](#)

Performing Common System Management Actions

The Oracle ILOM web interface provides an Actions panel on the Summary page that you can use to:

- View and change the state of commonly used system properties such as the power state and the Locator Indicator LED state on a managed device.
- Update the firmware image currently installed on the managed device.
- Launch the remote console feature or the x86 Oracle System Assistant.

 **Note:**

Oracle System Assistant is only available on Oracle's x86 servers.

For further details about initiating these commonly used host management actions from the Actions panel on the web interface Summary page, see these topics:

- [View and Modify the Device Power State From the Actions Panel \(Web\)](#)
- [View and Modify the Device Locator State From the Actions Panel \(Web\)](#)
- [Update the Device Firmware From the Actions Panel \(Web\)](#)
- [Launch the Remote Console From the Actions Panel \(Web\)](#)
- [Launch the x86 Oracle System Assistant](#)

View and Modify the Device Power State From the Actions Panel (Web)

The Power state property for the host server is viewable and configurable from the Actions panel in the web interface Summary page.

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify the power state on a managed device.

 **Note:**

Alternatively, you can modify the power state for a managed device from the Host Management > Remote Power Control page, or from the CLI `/System` target. For details about using these alternative methods to control the power state, see the topics in the Related Information section following this procedure.

1. To view the power state for a managed device, click System Information > Summary.

The current power state for the managed device appears in the Actions panel.

2. To modify the power state shown for a managed device, do one of the following:
 - **If Power state is set to ON in Actions Panel**, click the Turn Off button to perform a graceful shutdown of the operating system prior to powering off the host server.

 **Note:**

If the power to the host server fails to shut down, you can force a power shutdown by clicking Immediate Power Off on the Host Management Power Control page.

- **If Power state is set to Off in Actions Panel**, click the Turn On button to return power to the host server.

A prompt appears confirming that you want to proceed; click Yes to continue or No to cancel the action.

Related Information

- Controlling Host Power to Server

View and Modify the Device Locator State From the Actions Panel (Web)

The Locator Indicator state property for the host server is viewable and configurable from the Actions panel in the web interface Summary page.

Before You Begin

- Refer to the server documentation for information about the Locator Indicator. If your platform documentation does not mention a Locator Indicator, contact your Oracle service representative.

 **Note:**

Alternatively, you can view and modify the Locator Indicator state from the CLI / `System` target. For instructions, see the links in the Related Information section following this procedure.

1. To view the current Locator Indicator state on the managed device, click System Information > Summary.

The current Locator Indicator state for the managed device appears in the Actions panel.

2. To modify the state shown in the Actions panel for Locator Indicator, click the Turn On or Turn Off button for Locator.

A prompt appears asking you to confirm that you want to proceed; click Yes to continue or No to cancel the action.

Related Information

- Locate a Managed Device Using the Locator LED
- Configuring Host Server Management Actions

Update the Device Firmware From the Actions Panel (Web)

The System Firmware Update property for the host server is viewable and configurable from the Actions panel in the web interface Summary page.

Before You Begin

- If required by your platform, shut down the host operating system prior to updating the firmware image on the server SP.
- Admin (a) role privileges are required to update the system firmware.
- The firmware update process takes several minutes to complete. During this time, do not perform other Oracle ILOM tasks. When the firmware update is complete, the system will reboot.

Note:

Alternatively, you can launch the firmware update process from the ILOM Administration > Maintenance > Firmware Upgrade page. You can also launch the firmware update process from the Oracle ILOM CLI. For details, see the topics in the Related Information section following this procedure.

To initiate the firmware update process from the Actions panel on the web interface Summary page:

1. Determine the current firmware version installed on the server SP.

From the web interface, click System Information > Summary and view the System Firmware Version Installed value in the General Information table.

2. Open a new web browser tab or window and navigate to the following site to download the Oracle ILOM firmware image:

<http://support.oracle.com/>

For detailed instructions on downloading software updates from the My Oracle Support web site, see Oracle ILOM Firmware Versions and Download Methods.

Note:

Updating the system firmware image on a managed device to a prior firmware release is not recommended. However, if an earlier firmware release is required, Oracle ILOM will support the firmware update process to any prior firmware release that is available from the download site.

3. Place the firmware image on a server supporting one of the following protocols: TFTP, FTP, SFTP, SCP, HTTP, or HTTPS.

For web interface firmware updates, you should copy the image to the system on which the Oracle ILOM web browser is running.

4. To update the Oracle ILOM firmware image from the Actions panel in the web interface Summary page, click System Information > Summary, and do the following:
 - a. In the Actions panel, click the Update button for System Firmware Update. The Firmware Upgrade page appears.
 - b. Click Enter Upgrade Mode in the Firmware Upgrade page. An Upgrade Verification dialog box appears, indicating that other users who are logged in will lose their sessions when the update process is complete.
 - c. In the Upgrade Verification dialog box, click OK to continue. The Firmware Upgrade page appears.
5. Perform the following actions:
 - a. Specify the image location by performing one of the following:
 - Click Browse to select the location of the firmware image you want to install.
 - If supported on your system, click Specify URL. Then, in the text field, type the URL that will locate the firmware image.
 - b. Click the Upload button to upload and validate the file, and then wait for the file to upload and validate.
Click the Upload button to upload and validate the file, and then wait for the file to upload and validate.
The Firmware Verification page appears.
6. Enable any of the following options:
 - **Preserve Configuration** – Enable this option if you want to save your existing configuration in Oracle ILOM and restore that existing configuration after the update process is complete.
 - **Delay BIOS upgrade until next server power-off** – Enable this option if you want to postpone the BIOS upgrade until the next time the system reboots.

 **Note:**

The Delay BIOS upgrade option appears only for firmware updates on Oracle x86 servers.

 **Note:**

For Oracle x86 servers, Oracle ILOM prompts you to preserve the current BIOS properties on the managed device. If you answer Yes, Oracle ILOM will preserve the current BIOS properties after completing the firmware update. If you answer No, Oracle ILOM will set the BIOS properties to factory defaults after completing the firmware update.

7. Click Start Upgrade to start the upgrade process, or click Exit to cancel the process.
When you click Start Upgrade, the upgrade process begins, and a prompt to continue the process appears.
8. At the prompt, click OK to continue.

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

When the upload is complete, the system automatically reboots.

 **Note:**

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

9. Reconnect to the Oracle ILOM SP web interface. Click System Information > Summary to verify that the firmware version on the SP corresponds to the firmware version you installed.

Related Information

- Updating Oracle ILOM Firmware
- Recover From a Network Failure During Firmware Update
- Update the Server SP Firmware Image

Launch the Remote Console From the Actions Panel (Web)

Before You Begin

Review the graphical remote console first-time setup requirements:

- For systems that shipped with Oracle ILOM 3.2.x, refer to Using the Oracle ILOM Remote System Console Plus.
- For systems that shipped with Oracle ILOM 3.1 or 3.0, refer to Using the Oracle ILOM Remote System Console or Storage Redirection CLI.

A Remote Console Launch button appears in the Actions panel of the Oracle ILOM Summary page, which enables you to launch the graphical remote console feature. With the remote console, you can redirect the host system keyboard, video, mouse, and storage devices.

A text-based serial redirection feature is also available in Oracle ILOM. For more information about serial redirection, see Using Remote KVMS Consoles for Host Server Redirection.

1. To access the Actions panel in the web interface, click System Information > Summary.

The Actions panel appears in the upper right corner of the Summary page.

 **Note:**

Alternatively, the remote console can be launched in the web interface by clicking the Launch Remote Console button on the Remote Control > Redirection page.

2. Click the Remote Console Launch button.

If the web browser 32-bit JDK plug-in was not configured for first-time-use, the “Opening `jnlpgenerator.cli`” dialog appears. Prior to clicking OK to proceed, review the browser JDK plug-in configuration options described in the *Oracle ILOM Administrator's Guide for Configuration and Maintenance*.

The Oracle ILOM Remote System Console Plus window appears.

 **Note:**

If the system shipped with Oracle ILOM 3.1 or 3.0, the Oracle ILOM Remote System Console window appears.

The remote console window displays the host server desktop in its present state. For example:

- If the host server is powering-up, a set of boot messages appear.
- If the host server operating system is powered-on, a desktop log in dialog appears.
- If the host server is not powered-on, a blank screen appears.

Related Information

- Using Remote KVMS Consoles for Host Server Redirection
- Optionally Set a Lock Mode to Secure the Host Server Desktop

Launch the x86 Oracle System Assistant


Oracle System Assistant is a tool that offers features for provisioning servers, including operating system installation, firmware updates, RAID configuration, and more. For additional information about these features, refer to the administration guide for your x86 server.

Before You Begin

- The Launch option for Oracle System Assistant appears in Oracle ILOM only when Oracle System Assistant is present on the host x86 server.
- Power off the host operating system on the host server. If you do not power off the host OS prior to performing this procedure, Oracle ILOM will prompt you to power off the host before launching the Oracle System Assistant.
- When launching Oracle System Assistant, you will be prompted to launch a new remote console session. Therefore, prior to launching Oracle System Assistant, ensure that the setup requirements for launching and using the graphical remote console (JDK version, browser Java plug-in, and KVMS settings) are met. For more information about these requirements, see [Launch the Remote Console From the Actions Panel \(Web\)](#).
- The Admin (a) role is required in Oracle ILOM to launch Oracle System Assistant. The Console (c) role is required to launch the remote console.

This procedure provides both web and CLI instructions.

- To launch Oracle System Assistant, perform one of the following Oracle ILOM interface procedures:

Oracle ILOM Interface	Launch Oracle System Assistant Procedure
Web	<ul style="list-style-type: none"> • In the Actions panel, which is located in the System Information > Summary page, click the Launch button for Oracle System Assistant. One or more of the following prompts appear: Power off host prompt: This prompt appears only if the host server was not powered-off prior to performing this procedure. Click OK to power-off the host server. Launch a new remote console prompt: This prompt appears prior to launching the remote console. <div style="border: 1px solid #0070C0; padding: 10px; margin: 10px 0;"> <p> Note:</p> <p>You might encounter the following behavior: 1) an alert message appears stating "cannot get power state" and 2) a powered-off state is shown for Power in the Actions panel. If you encounter this behavior, it is because Oracle ILOM is temporarily unable to obtain the host server information. In this situation, click OK in the alert message to continue launching Oracle System Assistant. When you return to the Summary page, click Refresh to update the host power state shown in the Actions panel.</p> </div> <p>Oracle ILOM launches Oracle System Assistant in the Oracle ILOM Remote System Console (Plus) window.</p> <p>Refer to the x86 server administration guide for instructions for using the Oracle System Assistant.</p>
CLI	<ol style="list-style-type: none"> 1. In the Oracle ILOM CLI, type: <code>start /HOST/provisioning/system-assistant</code> The following prompt appears: <code>Are you sure that you want to start /HOST/ provisioning/system-assistant (y/n)?</code> 2. Type <code>y</code> to launch Oracle System Assistant (or type <code>n</code> to cancel the operation). Oracle ILOM launches Oracle System Assistant. Refer to the x86 server administration guide for instructions for using Oracle System Assistant.

Related Information

- Administration guide for Oracle x86 server, Oracle System Assistant

5

Applying Host and System Management Actions

Description	Link
Find links to Oracle ILOM configuration topics that describe how to set properties for host management actions.	<ul style="list-style-type: none">• Administering Host Management Configuration Actions
Find links to Oracle ILOM configuration topics that describe how to set properties for server management actions.	<ul style="list-style-type: none">• Administering System Management Configuration Actions

Related Information

- [Setting System Management Power Source Policies and Device Monitoring](#)
- [Maintaining x86 BIOS Configuration Parameters](#)
- [Configuring Host Server Management Actions](#)
- [Performing Oracle ILOM Maintenance and Configuration Management Tasks](#)

Administering Host Management Configuration Actions

Description	Link
Control rackmount power properties.	<ul style="list-style-type: none">• Controlling Host Power to Server
Control the next boot device.	<ul style="list-style-type: none">• Setting Next Boot Device on x86 Host Server
Enable SP diagnostics on a managed server.	<ul style="list-style-type: none">• Setting Diagnostic Tests to Run
Manage SPARC host boot, host domains, KeySwitch, and TPM properties.	<ul style="list-style-type: none">• Setting Host Control and Boot Properties on SPARC Host Server• Overriding SPARC Host Boot Mode• Managing SPARC Host Domains• Setting SPARC Host KeySwitch State• Setting SPARC Host TPM State

Administering System Management Configuration Actions

Description	Link
Back up and restore BIOS properties on an x86 managed server.	<ul style="list-style-type: none">• Maintaining x86 BIOS Configuration Parameters
Set system management policies on a managed device.	<ul style="list-style-type: none">• Setting System Management Power Source Policies and Device Monitoring
Back up and restore the Oracle ILOM configuration, and reset the server SP.	<ul style="list-style-type: none">• Performing Oracle ILOM Maintenance and Configuration Management Tasks

6

Real-Time Power Monitoring Through Oracle ILOM Interfaces

Description	Link
View power consumption metrics for a managed device using Oracle ILOM interfaces.	<ul style="list-style-type: none">• Monitoring Power Consumption
Learn about properties, hardware components, monitoring considerations, and instructions for viewing power allocation metrics for a managed device using Oracle ILOM interfaces.	<ul style="list-style-type: none">• Monitoring Power Allocations
View power statistics, power history metrics, and graphs using the Oracle ILOM interfaces.	<ul style="list-style-type: none">• Analyzing Power Usage Statistics• Comparing Power History Performance

Related Information

- [Setting Power Alert Notifications and Managing System Power Usage](#)

Monitoring Power Consumption

The Power Consumption properties, shown in the Oracle ILOM interfaces, enable you to acquire:

- Input power wattage value currently being consumed by a managed device.
- Maximum power wattage value a managed device is permitted to consume.
- Power consumption threshold wattages set for generating power event notifications.

For additional details about the power consumption properties presented by Oracle ILOM, see the following topics:

- [View Power Consumption Properties for a Managed Device](#)
- [Power Consumption Terminology and Properties](#)

View Power Consumption Properties for a Managed Device

Before You Begin

Review [Power Consumption Terminology and Properties](#).

- To view the power consumption properties from the SP web interface or CLI, do one of the following:
 - **From the SP web interface**, click Power Management > Consumption.
 - **From the SP CLI**, type the `show` command followed by the appropriate target and property.

For example, to view CLI power consumption properties for a single SP Oracle server, type one of the following:

- show /SP/powermgmt actual_power
- show /SP/powermgmt permitted_power
- show /SP/powermgmt threshold1\2

Where:

- 1|2 indicates the threshold number. Type **1** to view threshold 1, or type **2** to view threshold 2.

To view power consumption properties for PDomain *n* on a multi-domain SPARC server, type one of the following:

- show /Servers/PDomains/PDomain_n/SP/powermgmt actual_power
- show /Servers/PDomains/PDomain_n/SP/powermgmt permitted_power
- show /Servers/PDomains/PDomain_n/SP/powermgmt allocated_power

Related Information

- [Setting Power Alert Notifications and Managing System Power Usage](#)
- [Setting SP Power Limit Properties](#)
- [Set Advanced Power Capping Policy](#)

Power Consumption Terminology and Properties

- [Power Consumption Terminology](#)
- [Power Consumption Properties in Oracle ILOM Interfaces](#)

Table 6-1 Power Consumption Terminology

Terms	Applicable Function	Description
Real-time power monitoring	-	Oracle ILOM enables <i>real-time power monitoring</i> , within one second accuracy, by polling hardware interfaces (SP, power supply units (PSUs), and so forth) at any instance in time to present continuously updated power monitoring metrics in Oracle ILOM interfaces.
Power Consumption	-	<i>Power consumption</i> refers to either the input power consumed by the managed device or the output power provided by the PSUs.
-	<ul style="list-style-type: none"> • Input power • Output power 	<ul style="list-style-type: none"> • <i>Input power</i> is the power that is pulled into the chassis power supply units from an external power source. • <i>Output power</i> is the amount of power provided from the power supply units to the chassis components.
Power Consumption per managed device	-	The <i>power consumption</i> metric, appearing in Oracle ILOM interfaces, depends on the following hardware configurations:

Table 6-1 (Cont.) Power Consumption Terminology

Terms	Aplicable Function	Description
-	<ul style="list-style-type: none"> Rackmount 	<ul style="list-style-type: none"> <i>Server power consumption</i> is the sum of input power being consumed by the rackmount chassis power supplies.



Note:

CLI paths for Oracle's multi-domain SPARC systems are not included in the following table. To view power properties for a specific PDomain, append `/Servers/PDomains/PDomain_n/` to the beginning of the CLI paths listed.

Table 6-2 Power Consumption Properties in Oracle ILOM Interfaces

Power Metric Property	Managed Device	Description
Actual Power (<code>/SP/powermgmt actual_power</code>) or (<code>/System/Power actual_power_consumption</code>)	x86 SP SPARC SP	The read-only <i>Actual Power</i> property value, shown in Oracle ILOM interfaces, indicates the consumed power wattage by the managed server.
Target Limit (<code>/SP/powermgmt/budget powerlimit</code>)	x86 SP SPARC SP	<p>The read-only <i>Target Limit</i> property value, shown in Oracle ILOM interfaces, displays the current Target Limit value (wattage or percentage) set on the Oracle server.</p> <p><i>Important power monitoring considerations:</i></p> <ul style="list-style-type: none"> Oracle ILOM uses the set target limit value to determine the power budgeting parameters allowed for a server. Not all x86 servers will show a power management Target Limit property in the Oracle ILOM interfaces. When a Target Limit property is not supported by an x86 server, Oracle ILOM determines the power budgeting parameters for that server based on the power-consuming hardware components installed on the server. If the Target Limit property is supported (shown) in Oracle ILOM interfaces and a property value is not set, the property value <code>Not Configured</code> appears in the Oracle ILOM interfaces. <p>For more information about power budgeting or instructions for setting a Target Limit, refer to the Setting SP Power Limit Properties.</p>

Table 6-2 (Cont.) Power Consumption Properties in Oracle ILOM Interfaces

Power Metric Property	Managed Device	Description
Peak Permitted (/SP/powermgmt permitted_power) or (/System/Power max_permitted_power)	x86 SP SPARC SP	The read-only <i>Peak Permitted</i> property value, shown in Oracle ILOM interfaces, displays the maximum power wattage a managed device can consume: <ul style="list-style-type: none"> For an Oracle rackmounted server, the peak permitted value represents the maximum input power that the server can consume.
Event Notification Threshold <i>Default settings:</i> disabled <ul style="list-style-type: none"> Threshold 1 = 0 watts Threshold 2 = 0 watts (/SP/powermgmt threshold 1 2 = 0)	x86 SP SPARC SP	The user-defined <i>Notification Threshold</i> properties, shown in Oracle ILOM interfaces, display the power wattage value set to trigger an alert notification. When enabled, an alert notification is triggered by Oracle ILOM when the power consumption wattage on a managed device exceeds the user-defined threshold value. <p>Note: Event notifications generated by Oracle ILOM are dependent on whether email alert properties are properly configured in Oracle ILOM interfaces. For more information, refer to Setting Power Alert Notifications and Managing System Power Usage.</p>

Related Information

- Setting Power Consumption Alert Notifications

Monitoring Power Allocations

The Power Management Allocation Plan, shown in Oracle ILOM interfaces, can aid your efforts in planning an energy-efficient data center. The properties shown in the Allocation Plan enable you to effectively monitor and acquire the precise power metrics allocated to a single managed device, or the individual components installed on a managed device.

For more details about the power metric properties shown in the Allocation Plan, see the following topics:

- [Power Allocation Plan Properties per Managed Device](#)
- [Power Allocated Components and Monitoring Considerations](#)
- [View the Power Allocation Plan for a Managed Device](#)

View the Power Allocation Plan for a Managed Device

Before You Begin

- Review [Power Allocation Plan Properties per Managed Device](#)
 - Review [Power Allocated Components and Monitoring Considerations](#)
- To view the Power Allocation Plan properties from the SP web interface, click Power Management > Allocation.

The Power Allocation Plan for the managed device appears.

2. To view the Power Allocation Plan properties from the SP CLI, perform the following:

 **Note:**

CLI paths for SPARC multi-domain servers are not included in this step. To view power properties for a specific PDomain, append `/Servers/PDomains/PDomain_n/` to the beginning of the CLI paths listed below.

- View SP System Power Specification properties:
 - a. To view the Allocated Power and Peak Permitted power property values, type:
`show /SP/powermgmt/ allocated_power permitted_power`
 - b. To view property value for Target Limit (this property is not supported on all servers), type:
`show /SP/powermgmt/budget powerlimit`
 - c. To view the property for Power Supply Maximum, type:
`show /SP/powermgmt/ available_power`
- View SP Per Component Map properties:
 - a. To view a list of power allocated components configured on a managed server, type:
`show /SP/powermgmt/powerconf/`
 - b. To view power allocated property values for a specific server component, type:
`show /SP/powermgmt/powerconf/ component_type / component_name`

Where *component_type* is the name of the component category and *component_name* is the name of the component.

For example, to view the power allocated to a specific CPU, you would type:

```
show /SP/powermgmt/powerconf/CPU/CPU n
```

Where *n* is the installed location number of the CPU.

Related Information

- [Power Allocation Plan Properties per Managed Device](#)
- [Power Allocated Components and Monitoring Considerations](#)
- [Setting SP Power Limit Properties](#)
- [Setting SP Advanced Power Capping Policy to Enforce Power Limit](#)

Power Allocation Plan Properties per Managed Device

- [System Power Specification Properties \(Power Allocation\)](#)
- [Per Component Power Map Properties \(SP Power Allocation\)](#)

Table 6-3 System Power Specification Properties (Power Allocation)

Power Metric Property (read-only)	Managed Device	Description
Power Supply Maximum (/SP/powermgmt available_power)	x86 SP	The <i>Power Supply Maximum</i> property value, shown in Oracle ILOM interfaces, represents the maximum input power wattage that the power supplies are capable of drawing from the power outlets.
Peak Permitted (/SP/powermgmt permitted_power)	x86 SP SPARC SP	<p>The <i>Peak Permitted</i> property value, shown in Oracle ILOM interfaces, represents the maximum power wattage consumption guaranteed to the managed device. For instance:</p> <ul style="list-style-type: none"> For Oracle x86 and SPARC servers, the Peak Permitted property represents the maximum input power wattage that the server can consume at any instant. <p><i>Important monitoring considerations:</i></p> <ul style="list-style-type: none"> Not all x86 server SPs support the property for Target Limit in the Oracle ILOM interfaces. In these instances, the same property value (wattage) shown for Peak Permitted is derived by the power consuming hardware components installed on the managed server. For an Oracle server SP, Oracle ILOM derives the wattage value shown for Peak Permitted from the property values shown for Allocated Power and Target Limit. If the Target Limit property is not supported, Oracle ILOM derives the Peak Permitted property value from the power consuming hardware components installed on the managed server. <p>For further information about budgeting power that is consumed by a managed device, refer to Setting Power Alert Notifications and Managing System Power Usage.</p>
Allocated Power (/SP/powermgmt allocated_power)	x86 SP SPARC SP	<p>The <i>Allocated Power</i> property value, shown in Oracle ILOM interfaces, represents the maximum input power wattage allocated to a managed device. For example:</p> <ul style="list-style-type: none"> For an Oracle rackmounted server, the Allocated Power property value represents the total sum of the maximum power allocated to all installed chassis components and hot-pluggable components configured on the rackmount server.

Table 6-3 (Cont.) System Power Specification Properties (Power Allocation)

Power Metric Property (read-only)	Managed Device	Description
Target Limit (/SP/powermgmt/ budget powerlimit)	x86 SP SPARC SP	<p>The <i>Target Limit</i> property value, shown in Oracle ILOM interfaces, displays the power limit value (wattage or percentage) configured on the server.</p> <p><i>Important power monitoring considerations:</i></p> <ul style="list-style-type: none"> • Oracle ILOM uses the set power limit value to determine the power budgeting parameters allowed for a server. • When a power limit is not configured in Oracle ILOM, the read-only Target Limit property value <code>Not Configured</code> appears in the Power Allocation Plan. • Not all x86 server SPs support a Target Limit property in the Oracle ILOM interfaces. When a Target Limit property is not supported, Oracle ILOM will determine the Peak Permitted wattage value based on the power consuming hardware components installed on the managed server. <p>For more information about power budgeting or instructions for configuring a power limit, refer to <i>Setting Power Alert Notifications and Managing System Power Usage</i>.</p>

Table 6-4 Per Component Power Map Properties (SP Power Allocation)

Power Metric Property (read-only)	Managed Device	Description
Allocated Power (/SP/powermgmt allocated_power)	x86 SP SPARC SP	<p>The <i>Allocated Power</i> property value, shown in Oracle ILOM SP interfaces, represents the total sum of power wattage allocated to either: 1) a server component category (CPUs), or 2) an individual component installed on the server (MB_P0).</p>
Can be capped	x86 SP SPARC SP	<p>A Yes or No property value, per server component, appears in the Oracle ILOM SP web interface to indicate whether a power budget limit can be set for that server component.</p> <p>Note: If power budgeting (Target Limit property) is not supported by the server, the “Can be capped” property will not appear in the Power Management Allocation Plan.</p> <p>For further information about power budgeting, refer to <i>Setting Power Alert Notifications and Managing System Power Usage</i>.</p>

Power Allocated Components and Monitoring Considerations

- [Server SP Power Allocated Components](#)
- [Power Allocations Monitoring Considerations](#)

Table 6-5 Server SP Power Allocated Components

Server Component	Allocated Power	Applicable to Oracle x86 and SPARC Servers
All server power consuming components	• X	• X
CPUs	• X	• X
Memory Modules, such as DIMMs	• X	• X
Motherboard (MB)	• X	• X
Power Supply Units (PSUs)	• X	• X
Fans	• X	• X

Table 6-6 Power Allocations Monitoring Considerations

Power Allocated Components	Oracle ILOM Power Allocation Behavior
Oracle rackmounted servers	Power allocated to an Oracle rackmounted server is the maximum power the rackmount chassis components are capable of consuming. This value represents the maximum power wattage consumed by the processors, memory, I/O, fans, as well as the power loss across the power supplies. If the rackmount chassis contains slots for hot-pluggable components, the Power Allocated property value shown represents the maximum power wattage required for the most power-consuming component that can be installed in the hot-pluggable slot.
Hot-pluggable chassis components	Oracle ILOM automatically displays a pre-allocated maximum power value for any known hot-pluggable component that is installed in a hot-plug designated chassis slot location. For example: <ul style="list-style-type: none"> For rackmount hot-pluggable slots, Oracle ILOM displays the known maximum power wattage value required for a hot-pluggable component. To determine which components or slots in a rackmounted chassis are hot-pluggable, refer to the Oracle server documentation.
Chassis component categories	For chassis component categories that include multiple instances of the same component, Oracle ILOM presents the total sum of power allocated for a component category (fans), as well as the total sum of power allocated to an individual component (fan0).
Power supply unit (PSU)	Oracle ILOM automatically allocates power to the power supply to account for power losses between the wall outlet and the managed device.

Analyzing Power Usage Statistics

To help analyze the power consumed by a managed device, Oracle ILOM provides power statistic usage properties in bar graphs and tabular output. For more details, see these topics:

- [Rolling Average Power Statistics Graphs and Metrics](#)
- [View Power Statistics Bar Graphs and Metrics](#)

Rolling Average Power Statistics Graphs and Metrics

Oracle ILOM presents power metrics and bar graphs depicting a rolling average of power consumption in 15-, 30-, and 60-second intervals per managed device. These power usage metrics and bar graphs are particularly useful for analyzing energy consumption by a managed device.

View Power Statistics Bar Graphs and Metrics

- To display the power usage metrics and bar graph from the SP web interface, click Power Management > Statistics.

View the power wattage values and time intervals presented in the bar graph and in the Power History table.

Related Information

- [Power History Graphs and Metrics](#)
- [Set SP Power Target Limit Properties](#)
- [Setting SP Advanced Power Capping Policy to Enforce Power Limit](#)

Comparing Power History Performance

To help compare the power usage over time for a managed device, Oracle ILOM provides history statistics in bar graphs and tabular output. For more details, see:

- [Power History Graphs and Metrics](#)
- [View Power History Graphs and Metrics](#)

Power History Graphs and Metrics

Oracle ILOM presents history metrics and a series of bar graphs depicting the minimum, average, and maximum power consumption in:

- 1-hour intervals for a managed device
- 14-day intervals for a managed device
- 1-minute intervals in the last hour for a managed device
- 1-hour intervals in the last 14 days for a managed device

The power history metrics and graphs presented by Oracle ILOM are particularly helpful when comparing the best, average, and worst energy performance of a managed device.

View Power History Graphs and Metrics

1. To display the power history metrics and bar graphs from the SP web interface, click Power Management > History.
SP – You can toggle the graph display between a 1-hour interval and a 14-day interval.
2. To view additional power history sample sets from the SP web interface, click the links under the Sample Set column in the Power History table:

The Sample Set links enable you to view a bar graph depicting power consumption wattages in 1-minute intervals over the last hour, or 1-hour intervals over the last 14 days.

 **Note:**

The power history metrics and graphs presented by Oracle ILOM are not available from the SP CLI.

Related Information

- [Rolling Average Power Statistics Graphs and Metrics](#)
- [Setting SP Power Limit Properties](#)
- [Setting SP Advanced Power Capping Policy to Enforce Power Limit](#)

7

Troubleshooting Oracle ILOM Managed Devices

Description	Links
Resolve issues when establishing a management connection to Oracle ILOM.	<ul style="list-style-type: none">Network Connection Issues: Oracle ILOM Interfaces
Review a list of offline and online tools that you can use to observe and debug a managed system.	<ul style="list-style-type: none">Tools for Observing and Debugging System Behavior
Enable and run Oracle ILOM SP diagnostic tools.	<ul style="list-style-type: none">Enabling and Running Oracle ILOM Diagnostic Tools

Related Information

- [Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell](#)
- [Setting Diagnostic Tests to Run](#)
- [Suggested Resolutions for Network Connectivity Issues](#)
- [Oracle x86 Server Diagnostics Guide For Servers With Oracle ILOM](#)
- [Service manual for Oracle server](#)

Network Connection Issues: Oracle ILOM Interfaces

If you are experiencing difficulties establishing a network connection to the Oracle ILOM interfaces, refer to the following information for suggested resolutions:

Table 7-1 Troubleshooting Connectivity Issues

Problem	Suggested Resolution
Unable to access the Oracle ILOM web interface using an IPv6 address	Ensure that the IPv6 address in the URL is enclosed by brackets, for example: <code>https://[2001:db8:0:0:0:0:0:0]</code>
Unable to download a file using an IPv6 address	Ensure that the IPv6 address in the URL is enclosed by brackets, for example: <pre>load -source tftp://[2001:db8:0:0:0:0:0:0]/desktop.pkg</pre>

Table 7-1 (Cont.) Troubleshooting Connectivity Issues

Problem	Suggested Resolution
Unable to access Oracle ILOM using IPv6 from a network client	<p>If on a separate subnet, try the following:</p> <ul style="list-style-type: none"> • Verify that Oracle ILOM has a dynamic or static address (not just a Link-Local address). • Verify that the network client has an IPv6 address configured (not just a Link-Local address). <p>If on the same or a separate subnet, try the following:</p> <ul style="list-style-type: none"> • Ensure that the IPv6 State property is enabled on the Network Settings page in the Oracle ILOM web interface or under the <code>/SP/network/ipv6</code> target in the Oracle ILOM CLI. • Verify that the appropriate network service is enabled in Oracle ILOM: SSH, HTTP, or HTTPS. <p>In the web interface, click ILOM Administration > Connectivity to verify and change network connectivity settings.</p> <ul style="list-style-type: none"> • Use an industry-standard network diagnostic tool like IPv6 Ping or Traceroute to test the network connection to the managed device. Run Ping6 from the web interface or CLI.
Unable to access Oracle ILOM using IPv4 from a network client	<p>Ensure that the State property enabled on the Network Settings page in the Oracle ILOM web interface or under the <code>/SP/network</code> target in the Oracle ILOM CLI. Other suggestions for diagnosing IPv4 network issues include the following:</p> <ul style="list-style-type: none"> • Verify that a LAN connection to the physical management port (NET MGMT) is established. • Verify that the appropriate network service is enabled in Oracle ILOM: SSH, HTTP, or HTTPS. In the web interface, click ILOM Administration > Connectivity to verify and change network connectivity settings. • Use an industry-standard network diagnostic tool like IPv4 Ping or Traceroute to test the network connection to the managed device. Run Ping from the web interface or CLI.
Unable to access the Oracle ILOM web interface using the Microsoft Edge web browser	<p>Microsoft Edge users must upgrade browsers or upload custom certificate keys to use SSL in the Oracle ILOM web interface.</p>

Tools for Observing and Debugging System Behavior

A collection of online and offline diagnostic tools are provided with Oracle ILOM to assist system administrators and Oracle Services personnel who verify server behavior, troubleshoot problems, and perform repair or replacement service actions. For a list of Oracle ILOM diagnostic tools, their uses, and where to locate additional information about them, see the following table:

Table 7-2 Suggested Diagnostic Tools

Diagnostic Tool	For Details, See:
x86 host diagnostic tests	<ul style="list-style-type: none"> • Setting Diagnostic Tests to Run • Enabling x86 Diagnostics to Run at Boot
x86 processor non-maskable interrupt (NMI) for non-recoverable errors or to debug system status	<ul style="list-style-type: none"> • Generating x86 Processor Interrupt: Debugging System Status

Table 7-2 (Cont.) Suggested Diagnostic Tools

Diagnostic Tool	For Details, See:
SPARC host diagnostic tests	<ul style="list-style-type: none"> • Enabling Diagnostics to Run at Boot on Legacy SPARC Servers (M6, M5, T5, and Earlier)
Oracle ILOM Snapshot for taking service processor snapshots ¹	<ul style="list-style-type: none"> • Taking a Snapshot: Oracle ILOM SP State
Oracle ILOM open problems output for fault management	<ul style="list-style-type: none"> • Administering Open Problems • Protecting Against Hardware Faults: Oracle ILOM Fault Manager
Oracle ILOM Fault Management Shell	Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell
Oracle ILOM CLI for host operating system management	<ul style="list-style-type: none"> • Establishing a Host Serial Console Session to the Server (CLI) Supported Oracle ILOM CLI targets for launching a host console include: <code>SP/console</code> or <code>HOST/console</code> <p>Note: For Oracle's multi-domain SPARC servers, you can start a host console session for a PDomain from the following target: <code>/Servers/PDomains/PDomain_n/HOST/console</code></p>

¹ Oracle ILOM Snapshot is a diagnostic tool designed for authorized Oracle Services personnel.

Enabling and Running Oracle ILOM Diagnostic Tools

Oracle ILOM provides diagnostic tools to help resolve unexpected system performance or faulty component behavior on a managed device. For details on how to use these tools, see these topics:

- [Enabling x86 Diagnostics to Run at Boot](#)
- [Running the x86 HWDiag Tool within Oracle ILOM Diag Shell](#)
- [Generating x86 Processor Interrupt: Debugging System Status](#)
- [Enabling Diagnostics to Run at Boot on Legacy SPARC Servers \(M6, M5, T5, and Earlier\)](#)
- [Enabling Diagnostics to Run at Boot on Newer SPARC Systems \(M7 and T7 Servers\)](#)
- [Taking a Snapshot: Oracle ILOM SP State](#)

Enabling x86 Diagnostics to Run at Boot

In Oracle ILOM, you can enable diagnostics to test motherboard components, hard disk drives, ports, and slots on an Oracle x86 server. The following sections provide guidance on enabling diagnostics in Oracle ILOM:

- [Selecting a Diagnostic Test Level](#)
- [Enable UEFI Diagnostics to Run at Boot \(Web\)](#)
- [Enable PC-Check to Run at Boot \(Web\)](#)
- [Enable UEFI Diagnostics to Run at Boot \(CLI\)](#)

- [Enable PC-Check to Run at Boot \(CLI\)](#)

Selecting a Diagnostic Test Level

Before you enable diagnostics for an Oracle x86 server in Oracle ILOM, determine the level of diagnostics that you want to run. You can run a predefined test suite, or you can select specific tests to run from a list of options. The following table describes the available diagnostic levels:



Note:

To determine whether your server is running PC-Check or UEFI Diagnostics, refer to your server administration guide or to the Host Management > Diagnostics page in the Oracle ILOM web interface.

Table 7-3 Oracle x86 Server Diagnostic Levels

Diagnostic Tool	Diagnostic Level Descriptions
PC-Check	<p>Disabled (default) – PC-Check will not run diagnostic tests during host start-up. The server remains in normal operation mode.</p> <p>Enabled – PC-Check runs a predefined test suite without user intervention at host startup. Upon completion, the host will boot from the next device on the BIOS Boot Device Priority list. Use this mode to run quick diagnostic tests for first-time field installation or prior to installing mission-critical applications to verify system quality. The basic PC-Check tests typically take up to 5 minutes to complete.</p> <p>Extended – PC-Check runs a comprehensive test suite upon host startup. Use this mode after installing the system for the first time, after physically transporting the system, any time you add components, and prior to installing production operating systems and mission-critical applications. The extended PC-Check tests typically take 20 to 40 minutes to complete.</p> <p>Manual – The PC-Check diagnostic tests menu appears upon host startup. Use this mode to select tests from the PC-Check menu or to select predefined test suites through the Immediate Burn-in test menu. Test times depend on the tests selected.</p>
UEFI Diagnostics	<p>Disabled (default) – The server returns to normal operation mode. Diagnostic tests do not run.</p>

Table 7-3 (Cont.) Oracle x86 Server Diagnostic Levels

Diagnostic Tool	Diagnostic Level Descriptions
	<p>Enabled – The server boots automatically and executes a predefined test suite without user intervention. Test output is logged to the service processor directory (<code>/var/log/uefidiag/</code> or <code>/diag/log/uefidiag</code>), which can be viewed in the Oracle ILOM Fault Management Shell. After the diagnostic tests complete, the system automatically shuts down and returns to Disabled diagnostics mode. Use this mode as a quick test for first-time field installation and prior to installing mission-critical applications to verify system quality. These basic tests typically take between 20 minutes and 2 hours, depending on the system configuration.</p> <p>Extended – The server boots automatically and executes a comprehensive test suite without user intervention. Test output is logged to the service processor directory (<code>/var/log/uefidiag/</code> or <code>/diag/log/uefidiag</code>), which can be viewed in the Oracle ILOM Fault Management Shell. After the diagnostic tests complete, the system automatically shuts down and returns to Disabled diagnostics mode. Use this mode for first-time system installation, after physically transporting the system, any time you add components, and prior to installing production operating systems and mission-critical applications. These extended tests typically take between 30 minutes and 5 hours, depending on the system configuration.</p> <p>Manual – The server boots automatically to a test selection screen. In the test selection screen, you can specify the tests you want to run, or press Esc to issue UEFI Diagnostics commands in the UEFI shell environment instead. View the test output using a remote console, serial console, or a keyboard, video, and mouse connected to your system. You must manually return the diagnostics mode to Disabled once the tests are complete.</p>

Enable UEFI Diagnostics to Run at Boot (Web)

Before You Begin

- To diagnose Oracle x86 system hardware issues, you need the Reset and Host Control (r) role enabled.
- If you choose to run diagnostics in Manual mode, or if you want to monitor the progress of diagnostic tests in Enabled or Extended mode, do one of the following:
 - Start a host console redirection.

- Set up a serial console.
- Connect a keyboard, video, and mouse to your system.

 **Note:**

Alternatively, if you chose to run diagnostics in Enabled or Extended mode, the test output files are available for viewing by Oracle Service in Snapshot.

 **Note:**

To determine whether your server is running PC-Check or UEFI Diagnostics, refer to your server administration guide or to the Host Management > Diagnostics page in the Oracle ILOM web interface.

1. Power off the server:
 - a. In the Oracle ILOM web interface, click Host Management > Power Control.
 - b. In the Select Action list box select a Power Off option, and then click save.
2. From the Oracle ILOM web interface, click Host Management > Diagnostics.
The Diagnostics page appears.
3. If the host server is running Oracle ILOM 3.2.4, or a subsequent release, perform the following steps:
 - a. In the Mode list box, specify which diagnostic test level to run.
For details about the diagnostic levels, see [Selecting a Diagnostic Test Level](#).
 - b. Click Save.
The Start Diagnostics button is enabled.
 - c. Click Start Diagnostics.
An informational message about controlling diagnostics through the remote console application appears.
 - d. Click OK to clear the message and proceed with the diagnostic tests.
If you chose to run the diagnostic tests in Manual mode, the UEFI Diagnostics test selection screen appears on the host console.
The Diagnostics Status field indicates the progress of the diagnostic tests.
 - e. To safely disrupt the diagnostic tests, click Stop Diagnostics.

 **Caution:**

Do not disrupt the test progress by changing the server power state.

4. If the server is running Oracle ILOM 3.2.1 or 3.2.2, perform the following steps:
 - a. In the Run Diagnostics on Boot list box, specify the diagnostic test level to run.
For details about the diagnostic levels, see [Selecting a Diagnostic Test Level](#).

- b. Click Save.

If you chose to run the diagnostic tests in Manual mode, the UEFI Diagnostics test selection screen appears on the host console.

- c. If you ran UEFI Diagnostics in Manual mode, return the diagnostic test level to Disabled after the tests have concluded.

You must return the server to Disabled diagnostics mode before you can set the diagnostics mode to Enabled or Extended.

Enable PC-Check to Run at Boot (Web)

Before You Begin

- To diagnose Oracle x86 system hardware issues, you need the Reset and Host Control (r) role enabled.
- If you choose to run diagnostics in Manual mode, or if you want to monitor the progress of diagnostic tests in Enabled or Extended mode, do one of the following:
 - Start a host console redirection.
 - Set up a serial console.
 - Connect a keyboard, video, and mouse to your system.

Note:

Alternatively, if you chose to run diagnostics in Enabled or Extended mode, the test output files are available for viewing by Oracle Service in Snapshot.

1. From the Oracle ILOM web interface, click Host Management > Diagnostics.
The Diagnostics page appears.
2. In the Run Diagnostics on Boot list box, select the diagnostic test level to run.
For details about the diagnostic levels, see [Selecting a Diagnostic Test Level](#).
3. Click Save.
4. Power cycle the server:
 - a. Click Host Management > Power Control.
The Server Power Control page appears.
 - b. In the Select Action list box, select Power Cycle, and then click Save.
If you initiated a redirection session, the redirected display will initially show the host startup messages, and then it shows the progress of the diagnostic tests.
 - c. If a license agreement appears, click Enter to continue.
5. If you chose to run diagnostics in Manual mode, select Show Results Summary in the PC-Check menu to view the output files.
6. Return the server to normal operation mode by setting the Run Diagnostics on Boot property to Disabled.

Enable UEFI Diagnostics to Run at Boot (CLI)

Before You Begin

- To diagnose hardware issues on Oracle x86 systems, you need the Reset and Host Control (r) role enabled.
- If you choose to run diagnostics in Manual mode, or if you want to monitor the progress of diagnostic tests in Enabled or Extended mode, do one of the following:
 - Start a host console redirection.
 - Set up a serial console.
 - Connect a keyboard, video, and mouse to your system.
For details about launching a redirection session, see [Using Remote KVMs Consoles for Host Server Redirection](#).

 **Note:**

Alternatively, if you chose to run diagnostics in Enabled or Extended mode, the test output files are available for viewing by Oracle Service in Snapshot.

1. At the Oracle ILOM CLI prompt (->), type `stop /System` to power off the server.
2. Navigate to the `/HOST/diag` target:
cd /HOST/diag
3. If the host server is running Oracle ILOM 3.2.4, or a subsequent release, perform the following steps:
 - a. Issue the `set` command to specify the level of diagnostics to run, for example:

```
set mode=[disabled|enabled|extended|manual]
```


For details about diagnostics levels, see [Selecting a Diagnostic Test Level](#).
 - b. Issue the following `start` command to initiate the diagnostic tests:

```
start /HOST/diag
```


If you chose to run the diagnostic tests in Manual mode, the UEFI Diagnostics test selection screen appears on the host console.
 - c. Issue the following `show` command to view the progress of the diagnostic tests:

```
show /HOST/diag status
```
4. If the host server is running Oracle ILOM 3.2.1 or 3.2.2, perform the following steps:
 - a. Issue the following command to specify the diagnostic test level to run:

```
set mode=[disabled|enabled|extended|manual]
```


For details about diagnostics levels, see [Selecting a Diagnostic Test Level](#).
 - b. Issue the `show` command to view the progress of the diagnostic tests:

```
show /HOST/diag status
```

- c. Return the server to the normal operation mode by typing `set /HOST/diag mode=disabled`.

If you ran the diagnostics test in Enabled or Extended mode, the diagnostic mode on the server is automatically reset to Disabled.

Enable PC-Check to Run at Boot (CLI)

Before You Begin

- To diagnose hardware issues on Oracle x86 systems, you need the Reset and Host Control (r) role enabled.
- If you choose to run diagnostics in Manual mode, or if you want to monitor the progress of diagnostic tests in Enabled or Extended mode, do one of the following:
 - Start a host console redirection.
 - Set up a serial console.
 - Connect a keyboard, video, and mouse to your system.
For details about launching a redirection session, see [Using Remote KVMS Consoles for Host Server Redirection](#).

Note:

Alternatively, if you chose to run diagnostics in Enabled or Extended mode, the test output files are available for viewing by Oracle Service in Snapshot.

1. Navigate to the `/HOST/diag` target by typing:

```
cd /HOST/diag
```
2. Specify the diagnostic test level to run by issuing the following command:

```
set state=[disabled|enabled|extended|manual]
```

For details about diagnostics levels, see [Selecting a Diagnostic Test Level](#).
3. Power cycle the server.
 - a. Type: `stop /System`
 - b. Type: `start /System`

The diagnostic tests run upon powering on the server.
4. If you chose to run diagnostics in Manual mode, select Show Results Summary in the PC-Check menu to view the output files.
5. Return the server to normal operation mode by typing `set /HOST/diag state=disabled`.

Running the x86 HWdiag Tool within Oracle ILOM Diag Shell

The x86 HWdiag is a command-line utility that checks the status of a system and its components. You run the x86 HWdiag utility within the Oracle ILOM Diag shell.

 **Note:**

The x86 HWdiag utility is available for use only in Oracle ILOM 4.0.x and later releases. Check the x86 server product notes to see if this functionality is supported on your platform.

To run the x86 HWdiag tool, see the following procedure:

Run x86 HWdiag Tool (CLI)

1. At the Oracle ILOM CLI prompt, access the ILOM Diag shell, type:

```
start /SP/diag/shell
```

```
Are you sure you want to start /SP/diag/shell (y/n)? y
```

2. At the diag> prompt, issue a hwdiag command by using the following syntax:

```
diag> hwdiag [main_command] [subcommand]
```

For a list of supported HWdiag commands and options, view the HWdiag online help or refer to "Oracle ILOM Diagnostics" in the *Oracle x86 Servers Diagnostics and Troubleshooting Guide With Oracle ILOM 5.0*.

3. Choose any of the following ways to display help for hwdiag:
 - Type `help hwdiag` to display an overview of hwdiag options and main commands.
 - Type `help hwdiag -h` to display all hwdiag commands and their subcommands.
 - Type `help hwdiag -h -v` to display command structure with all options available by command.
 - Type `help hwdiag -h [command name]` to display help for a specific command.
4. Choose to use any of the following commands listed in the hwdiag command reference below:
 - `help` – Display the external commands available in the diag shell.
 - `echo` – Display information, for example, `echo $?`.
 - `exit` – Exit the diag shell.
 - `hwdiag` – Run hardware diagnostics.
 - `ls` – List the diagnostics log directories and files.
 - `cat` – Print the content of the diagnostics log files.

Generating x86 Processor Interrupt: Debugging System Status

Sending a nonmaskable interrupt (NMI) to the host operating system can cause the host to stop responding and wait for input from an external debugger. Therefore, you should use this feature only when requested to do so by Oracle Services personnel.

Generate a Nonmaskable Interrupt

Before You Begin

- Obtain permission from Oracle Services prior to performing this procedure.
- To generate an NMI from the Oracle ILOM interfaces, you need the Reset and Host Control (r) role enabled.
- The setting for generating a nonmaskable interrupt from Oracle ILOM might not be supported on all Oracle servers.

▲ Caution:

Depending on the host OS configuration, generating a nonmaskable interrupt (NMI) might cause the OS to crash, stop responding, or wait for external debugger input.

- To generate a processor interrupt, do one of the following:

- **From the Oracle ILOM web interface:**

1. Click Host Management > Diagnostics.

The Diagnostics page appears.

2. Click the Generate NMI button.

An NMI is sent to the host.

- **From the Oracle ILOM CLI, type:**

set /HOST/diag generate_host_nmi=true

For example:

```
-> set generate_host_nmi=true  
set 'generate_host_nmi' to 'true'
```

An NMI is sent to the host.

Enabling Diagnostics to Run at Boot on Legacy SPARC Servers (M6, M5, T5, and Earlier)

On an Oracle SPARC system, you can enable the diagnostic mode, specify triggers and the level of diagnostics, as well as the verbosity of the diagnostic output. For more information about legacy SPARC system diagnostics, see the following topics.

- [Enable Host Diagnostics to Run on Legacy SPARC Servers \(Web\)](#)
- [Enable Host Diagnostics to Run on Legacy SPARC Servers \(CLI\)](#)

Enable Host Diagnostics to Run on Legacy SPARC Servers (Web)

Before You Begin

- The Reset and Host control (⌘) role is required to modify the SPARC diagnostic properties in Oracle ILOM on SPARC systems.
- The Steps in this procedure are applicable to legacy SPARC servers such as M6, M5, T5 and some earlier T series servers.

To enable SPARC diagnostics tests to run when the system is powered on, do the following:

1. From the Oracle ILOM web interface, click Host Management > Diagnostics.
The Diagnostics page appears.
2. In the Trigger field, select one or more of the following triggers for running diagnostic tests:
 - **Power On** – Run diagnostics in the event of a routine power on, power cycle, or reset.

 **Note:**

This setting does not apply in the event of an AC power cycle, hardware change, or error-invoked reset.

- **HW Change** – Run diagnostics in the event of an AC power cycle, server top cover removal, or FRU (field-replaceable unit) replacement.
 - **Error Reset** – Run diagnostics in the event of an error-invoked reset.
3. In the Level list box for each trigger you selected in Step 2, select one of the following test levels:
 - **Min** – Run a basic suite of diagnostic tests.
 - **Max** – Run a basic suite of diagnostic tests plus extensive processor and memory tests.
 4. In the Verbosity list box for each trigger you selected in Step 2, select one of the following options for the verbosity of the diagnostic output:
 - **None** – Do not print output to the system console when diagnostics are run, unless a fault is detected.
 - **Min** – Print limited output to the system console when diagnostics are run.
 - **Normal** – Print a moderate amount of output to the system console when diagnostics are run, including the name and results for each test.
 - **Max** – Print output for each step in the diagnostic test process.
 - **Debug** – Print extensive debugging output to the system console when diagnostics are run, including the devices being tested and debugging output for each test.
 5. In the Mode list box, select one of the following options:
 - **Normal (default)** – Run diagnostic tests based on the triggers specified in Step 2.
 - **Off** – Disable all triggers for running diagnostic tests at boot.
 6. Click Save.

Enable Host Diagnostics to Run on Legacy SPARC Servers (CLI)

Before You Begin

- The Reset and Host control (r) role is required to modify the SPARC diagnostic properties in Oracle ILOM on SPARC systems.
- The Steps in this procedure are applicable to legacy SPARC servers such as M6, M5, T5 and some earlier T series servers.

To enable SPARC server diagnostics tests to run when the system is powered on, do the following:



Note:

CLI paths for multi-domain SPARC servers are not described in the following procedure. To set PDomain-specific diagnostics, append `/Servers/PDomains/PDomain_n/` to the beginning of the CLI paths listed below.

1. In the Oracle ILOM CLI, issue the set command to configure the host diagnostic trigger for running tests:

```
set /HOST/diag trigger= [none, power-on-reset, error-reset, all-reset]
```

where trigger = *[none, power-on-reset, error-reset, all-reset]*

- none — Do not run diagnostic tests.
- power-on-reset — Run diagnostics in the event of a routine power on, power cycle, or reset.



Note:

This setting does not apply in the event of an AC power cycle, hardware change, or error-invoked reset.

- error-reset — Run diagnostics upon any error-invoked power reset.
 - all-resets — Run diagnostics whenever a power reset occurs.
2. Set the diagnostic test level for the diagnostic trigger that you specified in Step 1:
 - If you specified `power-on-reset` or `all-resets`, type:

```
set /HOST/diag power_on_level= [min, max]
```
 - If you specified `error-on-reset` or `all-resets`, type:

```
set /HOST/diag error_reset_level= [min, max]
```where level = *[min, max]*
 - min — Run the minimum set of diagnostics to partially verify the health of the system.
 - max (default) — Run the maximum set of diagnostics to fully verify the health of the system.

3. Set the verbosity output for the diagnostic trigger that you specified in Step 1:
 - If you specified `power-on-reset` or `all-resets`, type:
`set /HOST/diag power_on_verbosity= [none, min, max, normal, debug]`
 - If you specified `error-on-reset` or `all-resets`, type:
`set /HOST/diag error_reset_verbosity= [none, min, max, normal, debug]`

where `verbosity = [none, min, max, normal, debug]`

 - `none` — Do not print output to the system console while diagnostics are run, unless a fault is detected.
 - `min` — Print limited output to the system console while diagnostics are run.
 - `max` — Print the full output to the system console while diagnostics are run, including the name and results for each test.
 - `normal (default)` — Print a moderate amount of output to the system console while diagnostics are ran.
 - `debug` — Print extensive debugging output to the system console while diagnostics are run, including device testing and debugging output for each test.
4. Set the diagnostic mode to either: 1) run the diagnostic tests at boot; or 2) disable the diagnostics tests from running at boot.
`set /HOST/diag mode=[off, default]`
where `mode = [off, default]`
 - `off` – Prevents the diagnostic test specified in Step 1 from running.
 - `(default)` – Runs the diagnostic test specified in Step 1.

Enabling Diagnostics to Run at Boot on Newer SPARC Systems (M7 and T7 Servers)

Oracle ILOM provides a set of server-specific diagnostic properties that enable system administrators to control whether system diagnostic tests are run at startup. For more information about SPARC platform diagnostics, see the following procedures, or refer to your platform-specific service manual.

- [Enable Host Diagnostics to Run on Newer SPARC Systems \(Web\)](#)
- [Enable Host Diagnostics to Run on Newer SPARC Systems \(CLI\)](#)
- [Enable SP Diagnostics to Run on Newer SPARC Systems \(Web\)](#)

Enable Host Diagnostics to Run on Newer SPARC Systems (Web)

Before You Begin

- The Reset and Host control (`r`) role is required to modify the SPARC diagnostic properties in Oracle ILOM on SPARC systems.
- The Steps in this procedure apply to newer SPARC servers such as T7, M7, and later SPARC series servers.

- Oracle ILOM firmware 3.2.5.5 or later.

To enable SPARC diagnostics tests to run, do the following:

1. From the Oracle ILOM web interface, click Host Management > Diagnostics.
The Diagnostics page appears.
2. In the Diagnostics page, specify the level and verbosity for each of the following properties:

- **Default** — Run diagnostics in the event of a routine power on, power cycle, or reset.

 **Note:**

This setting does not apply in the event of an AC power cycle, hardware change, or error-invoked reset.

- **HW Change** — Run diagnostics in the event of an AC power cycle, server top cover removal, or FRU (field-replaceable unit) replacement.
- **Error Reset** — Run diagnostics in the event of an error-invoked reset.

Levels:

The level determines the type of diagnostic tests that will run. You can set the Level property to the following:

- **Off** — Prevent POST from running
- **Min** — Run a basic suite of diagnostic tests
- **Max** — Run a basic suite of diagnostic tests, plus extensive processor and memory tests.

Verbosity:

The verbosity determines the amount of debugging output that is printed to the system console. You can set the Verbosity property to the following:

- **None** — Prevent debugging output from being printed to the system console.
- **Min** — Print a limited amount of debugging output.
- **Normal** — Print a moderate amount of debugging output, including test names and results.
- **Max** — Print all POST step debugging output.
- **Debug** — Print an extensive amount of debugging output, including names of devices being tested, as well as the debugging output for each test.

3. Click Save.

Enable Host Diagnostics to Run on Newer SPARC Systems (CLI)

Before You Begin

- The Reset and Host control (\mathcal{r}) role is required to modify the SPARC diagnostic properties in Oracle ILOM on SPARC systems.
- The Steps in this procedure apply to newer SPARC servers such as T7, M7, and later SPARC series servers.

- Oracle ILOM firmware 3.2.5.5 or later.

To enable SPARC server diagnostics tests to run, do the following:

 **Note:**

CLI paths for multi-domain SPARC servers are not described in the following procedure. To set PDomain-specific diagnostics, append `/Servers/PDomains/PDomain_n/` to the beginning of the CLI paths listed below.

- Issue the `set` command to configure the applicable host diagnostic properties:

```
set /HOST/diag default_level=[off, min, max]
default_verbosity=[none, min, normal, max debug]
error_level=[off, min, max] error_verbosity=[none, min,
normal, max debug] hw_change_level=[off, min, max]
hw_change_verbosity=[none, min, normal, max, debug]
```

where:

- `default_level` — determines the type of diagnostic tests that run in the event of a routine power on, power cycle, or reset. By default, the `default_level` is `off`.

 **Note:**

This setting does not apply in the event of an AC power cycle, hardware change, or error-invoked reset.

- `default_verbosity` — determines the amount of debugging output that is printed to the system console in the event of a routine power on. By default, the `default_verbosity` is `normal`.
- `error_level` — determines the type of diagnostic tests that run in the event of an error-invoked reset. By default the `error_level` is `max`.
- `error_verbosity` determines the amount of debugging output that is printed to the system console in the event of an error invoked reset. By default the `error_verbosity` is `normal`.
- `hw_change_level` — determines the type of diagnostic tests that run in the event of a server power cycle, server top cover removal, or FRU (field-replaceable unit) replacement. By default, the `hw_change_level` is `max`.
- `hw_change_verbosity` — determines the amount of debugging output that is printed to the system console in the event of a server power cycle, server top cover removal, or FRU (field-replaceable unit) replacement. By default, the `hw_change_verbosity` is `normal`.
where level = `[off, min, max]`
 - `off` — Prevent POST from running
 - `min` — Run a basic suite of diagnostic tests
 - `max` — Run a basic suite of diagnostic tests, plus extensive processor and memory tests.

where verbosity= [*none, min, normal, max, debug*]

- none — Prevent debugging output from being printed to the system console.
- min — Print a limited amount of debugging output.
- normal — Print a moderate amount of debugging output, including test names and results.
- max — Print all POST step debugging output.
- debug — Print an extensive amount of debugging output, including names of devices being tested, as well as the debugging output for each test.

For further property details, type: `help /Host/diag`

Enable SP Diagnostics to Run on Newer SPARC Systems (Web)

Before You Begin

- The Reset and Host control (`r`) role is required to modify the SPARC diagnostic properties in Oracle ILOM on SPARC systems.
- The Steps in this procedure apply to newer SPARC servers such as T7, M7, and later SPARC series servers.
- Oracle ILOM firmware version 3.2.5.5 or later.

To enable SPARC diagnostics tests to run, do the following:

1. Navigate to the SP Diagnostic properties:

- Web:
In the Oracle ILOM web interface, click System Management > Diagnostics.
The Diagnostics page appears.
- CLI
In the CLI, type: `cd /SP/diag`

2. Perform one of the following:

- Web:
In the Diagnostics page, configure the following properties and click Save.
 - **Default Level** [*Off (default), Min, or Max*] — Specify the appropriate diagnostic behavior in the event of a routine server power cycle (power off/on) or a server reset.

Note:

The POST Default Level property does not apply to error-invoked resets or hardware change events.

- **HW Change** [*Off, Min, or Max (default)*] — Specify the appropriate diagnostic behavior in the event of a server power-cord-cycle, server top cover removal, or FRU (field-replaceable unit) replacement.

 **Note:**

A server power-cord-cycle refers to when the power cords are removed, replaced, or when the power is first applied to server.

where: [Off, Min, and Max]

- **Off** — Prevent POST from running
- **Min** — Run a basic suite of diagnostic tests
- **Max** — Run a basic suite of diagnostic tests, plus extensive processor and memory tests.

- **CLI:**
In the CLI, issue the `set` command to configure the applicable host diagnostic properties:

```
set default_level= [off, min, max] hw_change= [off, min, max]
```

For further property details, type: `help /sp/diag`

Taking a Snapshot: Oracle ILOM SP State

 **Caution:**

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

The Snapshot feature in Oracle ILOM enables you to collect information about the current state of the service processor (SP). This information can include environmental data, logs, and information about field-replaceable units installed on the server. In addition, you can use Snapshot to run diagnostics on the host and capture the diagnostics log files.

The output from Snapshot is saved as a standard zip file or an encrypted zip file to a location you specify.

To use the Snapshot feature, see the following procedures:

- [Take a Snapshot of the Oracle ILOM SP State \(Web\)](#)
- [Take a Snapshot of the Oracle ILOM SP State \(CLI\)](#)
- [Decrypt an Encrypted Snapshot Output File](#)
- [Transfer Snapshot Output to Remote Console Over SSH Connection](#)

Take a Snapshot of the Oracle ILOM SP State (Web)

Before You Begin

- The Admin (a) role is required to collect SP data using the Snapshot feature.

 **Caution:**

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

1. From the Oracle ILOM web interface, click ILOM Administration > Maintenance > Snapshot.

From the Oracle ILOM web interface, click ILOM Administration > Maintenance > Snapshot.

The Snapshot page appears.

2. In the Data Set list box, select one of the following options:

In the Data Set list box, select one of the following options:

- Normal – Collect information about Oracle ILOM, the host operating system, and the hardware configuration.
- FRUID – Collect information about installed FRUs, in addition to the data set collected for Normal. The FRUID option enables Oracle Services personnel to analyze data in a binary format about FRUs.
- Full (may reset the host) – Collect the maximum amount of data from the host, and initiate diagnostics on the host. This option could cause the server to reset.
- Custom – Specify which of the following data sets to capture:
 - Oracle ILOM data
 - Hardware data
 - Diagnostic data

 **Note:**

This option might require a host reset.

- Basic OS data
 - FRUID data
3. Configure the following output properties:
 - Collect Only Log Files From Data Set – Enable (select) this option to collect only log files. Disable (deselect) this option to capture log files and additional information about the SP state.
 - Encrypt Output File – Enable (select) this option to encrypt the output file. When encryption is enabled, you are prompted for an encryption passphrase. To decrypt an encrypted output file, you will need to know the passphrase.

Deselect this option to produce a non-encrypted output file. To decrypt an encrypted output file, see [Decrypt an Encrypted Snapshot Output File](#).

4. In the Transfer Method list box, select one of the following options:

In the Transfer Method list box, select one of the following options:

- **Browser** – Specify the output destination in a browser window.
 - **SFTP** – Specify the SFTP host, your user name and password on the host, and the output file destination.
 - **FTP** – Specify the FTP host, your user name and password on the host, and the output file destination.
 - **FTPS** – Specify the FTPS host, your user name and password on the host, and the output file destination.
 - **TFTP** – Specify the TFTP host and the output file destination.
 - **HTTP** – Specify the HTTP host, your user name and password on the host, and the output file destination.
 - **HTTPS** – Specify the HTTPS host, your user name and password on the host, and the output file destination.
5. Click Run.
- Click Run.
- When the Snapshot is complete, the Save As dialog box appears prompting you to save the output file.
6. Specify the output directory in the Save As dialog box, and then click OK.

Take a Snapshot of the Oracle ILOM SP State (CLI)

Caution:

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

Before You Begin

- The Admin (a) role is required to collect SP data using the Snapshot feature.
1. In the Oracle ILOM CLI, issue the following command to specify what kind of data the snapshot utility should collect:
- In the Oracle ILOM CLI, issue the following command to specify what kind of data the snapshot utility should collect:
- ```
set /SP/diag/snapshot dataset= value
```
- where *value* can be one of the following:
- `normal` – Collect information about Oracle ILOM, host operating system, and hardware configuration.
  - `normal-logonly` – Collect only log files.
  - `FRUID` – Collect information about installed FRUs, in addition to the data set collected for Normal.
  - `fruid-logonly` – Collect only log files.
  - `full` – Collect the maximum information about the server. This option could cause the server to reset.



- `full-logonly` – Collect only log files.
2. To specify whether the snapshot data should be encrypted, type:  
To specify whether the snapshot data should be encrypted, type:  
**set /SP/diag/snapshot encrypt\_output=** [true|false]

 **Note:**

When the `encrypt_output` property is set to `true`, you must type an encryption password at the prompt in order to start the data collection. Later, you must type an encryption password at the prompt in order to decrypt the output file. To decrypt an encrypted output file, see [Decrypt an Encrypted Snapshot Output File](#).

3. To start the data collection, type:  
To start the data collection, type:  
**set /SP/diag/snapshot dump\_uri=protocol://username:password@host/directory**  
where the transfer `protocol` can either be: `sftp`, `tftp`, `ftp`, `ftps`, `http`, or `https`.  
For example, to store the snapshot information via `ftp` in a directory named `data` on the host, type:  
**set /SP/diag/snapshot dump\_uri=ftp://username:mypasswd@host-ip-address/data**

 **Note:**

The *directory* is relative to the user's login; therefore, in the previous example, the full path to `data` is probably `/home/username/data`.

## Decrypt an Encrypted Snapshot Output File

 **Note:**

The following procedure does not apply to the SSH Snapshot operation method.

1. Using a terminal window that supports `openssl` commands, navigate to the directory that contains the Snapshot output file.
2. Issue the decryption command:
  - If the host server is running Oracle ILOM 3.2.4, or a subsequent release, type:  
**openssl aes-128-cbc -d -md sha1 -in encryptedSnapshotFilename.zip.e -out snapshotFilename.zip**
  - If the host server is running Oracle ILOM 3.2.1 or 3.2.2, type:  
**openssl aes-128-cbc -d -in encryptedSnapshotFilename.zip.e -out snapshotFilename.zip**
3. When prompted, enter the encryption passphrase.

## Transfer Snapshot Output to Remote Console Over SSH Connection

As of Oracle ILOM firmware version 4.0.2, system administrators can choose to use the SSH Snapshot feature to transfer all Snapshot data directly to the client console over an established SSH session, rather than the conventional method of transferring the Snapshot data to a destination server over a separate network protocol like the tftp, sftp, and so on. With the SSH Snapshot feature, a non-text version of the output data is typically archived to a specified file destination on the remote host client system. The initiation of the SSH Snapshot operation is limited to a scripted or automated retrieval process where the encrypted data transfer is passed along during the setup of the SSH session.

### Before You Begin

- The Admin (a) role is required to configure the Snapshot property in Oracle ILOM.

To initiate the creation of a Snapshot and have its contents (raw data) redirected to a file over an existing SSH session, follow this procedure:

- On a remote host client system, open a command-line interface and type:  
On a remote host client system, open a command-line interface and type:
  - `l> ssh -l root [IP_or_hostname of Oracle ILOM SP] set -script /SP/diag/snapshot dump_uri=console > [destination_file_name].zip`

#### Note:

The `-script` command, when used, eliminates all system prompts by answering Yes to all Snapshot related collection prompts.

#### Note:

The encryption (`encrypt_output=`) option is not supported since the SSH Snapshot data is encrypted over the established SSH channel.

Where:

- `ssh -l root [IP_or_hostname of Oracle ILOM SP]` is the ssh connection info used to initiate the ssh session from the remote client system
- `set /SP/diag/snapshot dump_uri=console` is the CLI command that is passed along to initiate the snapshot collection
- `-script` is an optional command that can be used to eliminate system prompts during the Snapshot operation. When this command is used, all system related prompts are answered Yes during the Snapshot operation.
- `>` is the character symbol used to redirect the output to the destination file name
- `[destination_file_name].zip` is the file name on the client that will store the resulting Snapshot data output. Note that the .zip file extension is required to match the data format.

# 8

## Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell

Description	Links
Learn about hardware fault notifications, corrective action, and auto clearing of faults.	<ul style="list-style-type: none"><li><a href="#">Protecting Against Hardware Faults: Oracle ILOM Fault Manager</a></li></ul>
Launch and run fault management commands from the Oracle ILOM Fault Management Shell.	<ul style="list-style-type: none"><li><a href="#">Oracle ILOM Fault Management Shell</a></li><li><a href="#">Using fmadm to Administer Active Oracle Hardware Faults</a></li><li><a href="#">View Information About Active Faulty Components (fmadm faulty)</a></li><li><a href="#">Using fmdump to View Historical Fault Management Logs</a></li><li><a href="#">Using fmstat to View the Fault Management Statistics Report</a></li></ul>

### Related Information

- *Oracle x86 Server Diagnostics Guide For Servers With Oracle ILOM*
- Service manual for the Oracle server

## Protecting Against Hardware Faults: Oracle ILOM Fault Manager

The Fault Manager in Oracle ILOM is intended to help with problems that might occur on an Oracle ILOM managed device. For instance, the Fault Manager detects and interprets errors and determines whether a fault or defect is present on a managed system. When a determination is made, the Fault Manager issues a list of hardware components that might be the cause of the problem.

For additional information about how Oracle ILOM helps to enhance uptime when hardware faults are detected on a device, see:

- [Hardware Fault Notifications](#)
- [Hardware Fault Corrective Action](#)
- [Fault Events Cleared: Repaired Hardware](#)

### Hardware Fault Notifications

Notifications indicating that a hardware fault or defect has been diagnosed appear in the Open Problems tabular output, which is viewable from the Oracle ILOM interfaces. In addition to the hardware fault notifications provided in the Open Problems output, the Fault Manager also logs event messages to the event log and the Fault Management logs. You can view the

event log from the Oracle ILOM interfaces. The Fault Management logs are viewable from the Oracle ILOM Fault Management Shell.



**Note:**

You can also configure notification of fault events by using the Simple Network Management Protocol (SNMP) or Simple Mail Transfer Protocol (SMTP). For SNMP configuration details, refer to [Configuring SNMP Settings in Oracle ILOM](#). For SMTP configuration details, refer to the [Configure SMTP Client for Email Alerts](#).

## Hardware Fault Corrective Action

When you are notified of a diagnosed problem, always consult the recommended knowledge article for additional details. An [http://](#) reference is provided to the recommended knowledge article in the event notification in the Open Problems output, and in the event messages in the log files.

## Fault Events Cleared: Repaired Hardware

Fault events and notifications in Oracle ILOM are automatically cleared when the repaired or replaced resource is associated with a field-replaceable unit (FRU). However, when a repaired or replaced resource is not associated with a FRU, Oracle ILOM is unable to detect the change; therefore, the fault event notification is not automatically cleared in the Open Problems output or in the log files. For information about clearing fault events in Oracle ILOM for undetected repairs or replacements, see [Clearing Faults for Repairs or Replacements](#).

## Oracle ILOM Fault Management Shell

The Oracle ILOM Fault Management Shell enables system administrators and Oracle Services personnel to view and manage fault activity on a managed device.

For further information about how to use the Oracle ILOM Fault Management Shell, see these topics:

- [Fault Management Terminology](#)
- [Launch a Fault Management Shell Session \(CLI\)](#)

## Fault Management Terminology

Term	Description
Proactive self-healing	<i>Proactive self-healing</i> is a fault management architecture and methodology for automatically diagnosing, reporting, and handling software and hardware fault conditions. Proactive self-healing reduces the time required to debug a hardware or software problem and provides the system administrator or Oracle Services personnel with detailed data about each fault. The architecture consists of an event management protocol, the Fault Manager, and fault-handling agents and diagnosis engines.
Diagnosis engines	The fault management architecture, in Oracle ILOM, includes <i>diagnosis engines</i> that broadcast fault events for detected system errors. For a list of diagnosis engines supported in the fault management architecture for Oracle ILOM, see <a href="#">fmstat Report Example and Description</a> .
Health states	Oracle ILOM associates the following <i>health states</i> with every resource for which telemetry information has been received. The possible states presented in Oracle ILOM interfaces include: <ul style="list-style-type: none"> <li>• ok – The hardware resource is present in the chassis and in use. No known problems have been detected.</li> <li>• unknown – The hardware resource is not present or not usable, but no known problems are detected. This management state can indicate that the suspect resource is disabled by the system administrator.</li> <li>• faulted – The hardware resource is present in the chassis but is unusable since one or more problems have been detected. The hardware resource is disabled (offline) to prevent further damage to the system.</li> <li>• degraded – The hardware resource is present and usable, but one or more problems have been detected. If all affected hardware resources are in the same state, this status is reflected in the event message at the end of the list. Otherwise, a separate health state is provided for each affected resource.</li> </ul>
Fault	A <i>fault</i> indicates that a hardware component is present but is unusable or degraded because one or more problems have been diagnosed by the Oracle ILOM Fault Manager. The component has been disabled to prevent further damage to the system.
FRU	A <i>FRU</i> is a field-replaceable unit (such as a drive, memory DIMM, or printed circuit board).
CRU	A <i>CRU</i> is a customer-replaceable unit.

Term	Description
Universal unique identifier (UUID)	A <i>UUID</i> is used to uniquely identify a problem across any set of systems.

## Launch a Fault Management Shell Session (CLI)

### Before You Begin

- Admin (a) role privileges are required to launch the Fault Management Shell from the Oracle ILOM CLI.

To launch the Oracle ILOM Fault Management Shell, from the Oracle ILOM CLI, do the following:

1. From the Oracle ILOM CLI, type the following command to launch the Oracle ILOM Fault Management Shell:

```
start /SP/faultmgmt/shell
```

The following Fault Management Shell command prompt appears:

- `faultmgmtsp>`

#### Note:

After you start the Fault Management Shell and until you exit the Fault Management Shell, you can issue only commands that are specific to the Fault Management Shell.

2. At the `faultmgmtsp>` prompt, issue any of the following Fault Management Shell commands:

- `fmadm` – Display faulty components or clear faults for undetected repairs or replacements. See [Using `fmadm` to Administer Active Oracle Hardware Faults](#) for more details.
- `fmdump` – View historical fault management activity. See [Using `fmdump` to View Historical Fault Management Logs](#) for more details.
- `fmstat` – View a statistical report of fault management operations. See [Using `fmstat` to View the Fault Management Statistics Report](#) for more details.

3. To display information describing a Fault Management Shell command, type:

```
help [command]
```

where *command* can be one of the following:

- `fmadm`
- `fmdump`
- `fmstat`

4. To exit the Fault Management Shell, , type:

```
exit
```

 **Note:**

To issue standard Oracle ILOM CLI commands, you must first exit the Fault Management Shell.

## Related Information

- [Using `fmadm` to Administer Active Oracle Hardware Faults](#)
- [Using `fmdump` to View Historical Fault Management Logs](#)
- [Using `fmstat` to View the Fault Management Statistics Report](#)

## Using `fmadm` to Administer Active Oracle Hardware Faults

Use the `fmadm` utility in the Fault Management Shell to view and manage active Oracle hardware faults that are conventionally maintained by the Oracle ILOM Fault Manager. For further details on how to view and manage fault behavior using the `fmadm` utility, see these topics:

- [View Information About Active Faulty Components \(`fmadm faulty`\)](#)
- [Clearing Faults for Repairs or Replacements](#)

### View Information About Active Faulty Components (`fmadm faulty`)

 **Note:**

For Oracle hardware customers, the recommended method for viewing active information about faulty components is to view the health state of a component in the Open Problems tabular output, which is provided in the Oracle ILOM CLI and web interface.

To view information about active faulty components from the Oracle ILOM Fault Management Shell, do the following:

1. From the Oracle ILOM CLI, launch the Fault Management Shell, as described in [Launch a Fault Management Shell Session \(CLI\)](#).

The `faultmgmtsp>` prompt appears.

2. To view information about active faulty hardware components reported for a managed device, type:

To view information about active faulty hardware components reported for a managed device, type:

```
fmadm faulty display_option
```

where `display_option` can be one of the following:

- `-a` – Show active faulty components, type:
- `-f` – Show active faulty FRUs.
- `-r` – Show active fault FRUs and their fault management states.

- `-s` – Show a one-line fault summary for each fault event.
  - `-u uuid` – Show fault diagnosis events that match a specific universal unique identifier (`uuid`).
3. When applicable, refer to the `http://` referenced knowledge article in the `fmadm` faulty output for further instructions for resolving a reported problem.

#### Related Information

- [Fault Management Terminology](#)
- [Clear Faults for Undetected Replaced or Repaired Hardware Components](#)
- [Administering Open Problems](#)

## Clearing Faults for Repairs or Replacements

After you replace or repair a faulted component on a managed device, the Oracle ILOM Fault Manager automatically detects the repair or replacement and clears the associated fault message from the system. However, if the replaced or repaired hardware component is not associated with a FRU serial number, the corrective service action is not detected by Oracle ILOM, nor are the fault event messages associated with the undetected repair cleared from the Oracle ILOM interfaces.

You can manually clear fault messages for undetected repair or replacement service actions by issuing the appropriate `fmadm` repair commands in the Oracle ILOM Fault Management Shell. For more information, see these topics:

- [fmadm Command Usage and Syntax](#)
- [Clear Faults for Undetected Replaced or Repaired Hardware Components](#)

### `fmadm` Command Usage and Syntax

<b>fmadm Repair Command</b>	<b>Use to:</b>
<code>acquit [fru cru ]</code>	<p>Notify the Oracle ILOM Fault Manager that the specified faulted component is not to be considered suspect in any fault events that have been detected. The <code>fmadm</code> <code>acquit</code> command should be used only at the direction of a documented Oracle hardware repair procedure.</p> <p><b>Syntax example:</b></p> <p>To instruct the Fault Manager to ignore a suspect fan module in a rackmounted server chassis, type:</p> <pre>fmadm quit /SYS/FANBD/FMn</pre>
<code>acquit uuid</code>	<p>Notify the Oracle ILOM Fault Manager that the faulted event identified by the <code>uuid</code> resource can be safely ignored. The <code>fmadm</code> <code>acquit</code> command should be used only at the direction of a documented Oracle hardware repair procedure.</p> <p><b>Syntax example:</b></p> <p>To instruct the Fault Manager to ignore the event identified by 6d76a0f4-b5f5-623c-af8b-9d7b53812ea1, type:</p> <pre>fmadm quit 6d76a0f4-b5f5-623c-af8b-9d7b53812ea1</pre>



fmadm Repair Command	Use to:
<pre>repaired [fru cru]</pre>	<p>Notify the Oracle ILOM Fault Manager that the specified field-replaceable unit or customer-replaceable unit has been repaired. The <code>fmadm repaired</code> command should be used in those cases where the Oracle ILOM Fault Manager is unable to detect the repaired FRU.</p> <p><b>Syntax example:</b></p> <p>To notify the Fault Manager that a fan module in a rackmounted server chassis has been repaired, type:</p> <pre>fmadm repaired /SYS/FANBD/FMn</pre>
<pre>replaced [fru cru]</pre>	<p>Notify the Oracle ILOM Fault Manager that the specified faulted field-replaceable unit or customer-replaceable unit has been replaced. This command should be used in those cases where the Oracle ILOM Fault Manager is unable to detect the replacement.</p> <p><b>Syntax example:</b></p> <p>To notify the Fault Manager that a fan module in a rackmounted server chassis has been replaced, type:</p> <pre>fmadm replaced /SYS/FANBD/FMn</pre>

## Clear Faults for Undetected Replaced or Repaired Hardware Components

### Before You Begin

- Review [fmadm Command Usage and Syntax](#).
- If a fault event is cleared before the required corrective service action for the faulty component is completed, the Oracle ILOM Fault Manager diagnoses the fault and displays the fault event in the Oracle ILOM Open Problems table and in the Oracle ILOM Fault Management log files again.

To clear faults for undetected hardware repairs or replacements from the Oracle ILOM Fault Management Shell, do the following:

1. From the Oracle ILOM CLI, launch a Fault Management Shell, as described in [Launch a Fault Management Shell Session \(CLI\)](#).  
The `faultmgmtsp>` prompt appears.
2. Identify and display information about active suspect components.  
See [View Information About Active Faulty Components \(fmadm faulty\)](#) for more details.
3. Type one of the following `fmadm` commands to manually clear a fault:
  - `fmadm replaced [fru|cru]` – A suspect component has been replaced or removed.
  - `fmadm repaired [fru|cru]` – A suspect component has been physically repaired to resolve the reported problem. For example, a component has been reseated or a bent pin has been fixed.
  - `fmadm acquit [fru|cru] [uuid]` – A suspect component or `uuid` resource is not the cause of the problem.  
Where `[fru|cru]` `[uuid]` appears, type the system path to the suspect chassis FRU or CRU, or type the associated universal unique identifier (`uuid`) for the resource reported in the problem.

 **Note:**

A replacement takes precedence over a repair, and both replacement and repair take precedence over acquittal. Thus, you can acquit a component and subsequently repair it, but you cannot acquit a component that has already been repaired.

For syntax descriptions and examples, see [fmadm Command Usage and Syntax](#).

- To display the exit code for the last executed fault management command, type:

```
echo $?
```

One of the following echo codes appears:

Code	Description
0	Successful completion.
1	An error occurred. Errors can include a failure to communicate with Oracle ILOM and insufficient privileges to perform the requested operation.

#### Related Information

- [Fault Management Terminology](#)
- [View Information About Active Faulty Components \(fmadm faulty\)](#)
- [Administering Open Problems](#)

## Using `fmdump` to View Historical Fault Management Logs

The Oracle ILOM Fault Manager maintains historical information about system problems in two sets of log files for use by system administrators and Oracle Services personnel. A log file set can consist of active system events together with a number of older system events.

- [Log File Display Commands and Log Descriptions](#)
- [View Fault Management Log Files \(fmdump\)](#)

### Log File Display Commands and Log Descriptions

Display Command	Target Log	Description
fmdump	Fault log	The <i>fault management fault log</i> records human-readable fault diagnosis information and problems possibly related to the fault symptoms.  A time stamp and description is provided for each recorded event.

Display Command	Target Log	Description
fmdump -e	Error log	<p>The <i>fault management error log</i> records error telemetry and the symptoms of problems detected by the system. For each recorded problem, the following information is provided:</p> <ul style="list-style-type: none"> <li>• A time stamp for when the problem was detected.</li> <li>• A universal unique identifier (UUID) that uniquely identifies a particular problem across any set of systems.</li> <li>• An http:// identifier that provides access to a corresponding knowledge article posted on the Oracle support web site.</li> </ul>

 **Caution:**

Do not base administrative service actions on content in the fault management log files, but rather on the active `fmadm faulty` output. Because the fault management log files contain historical events, the information about faults and defects in the log files should not be considered active.

## View Fault Management Log Files (`fmdump`)

### Before You Begin

- Review [Log File Display Commands and Log Descriptions](#).

To view the fault management log files from the Oracle ILOM Fault Management Shell, do the following:

1. From the Oracle ILOM CLI, launch a Fault Management Shell, as described in [Launch a Fault Management Shell Session \(CLI\)](#)

The `faultmgmtsp>` prompt appears.

2. Type one of the following `fmdump` commands to display the contents of a fault management log file set:
  - `fmdump` – Display the fault log.
  - `fmdump -u uuid`– Display a fault log for a specific universal unique identifier (*uuid*).
  - `fmdump -e` – Display the error log.

 **Note:**

For the fault log, in particular, it is important to recognize that `fmdump` shows all problems ever diagnosed and is not limited to active problems diagnosed. To view active faults only, issue the `fmadm faulty` command.

3. To rotate the log display, do one of following:
  - To rotate the fault log display, type:  
`fmadm rotate fltlog`
  - To rotate the error log display, type:  
`fmadm rotate errlog`
4. To display the exit code for the last executed fault management command, type:  
`echo $?`

One of the following echo codes appears:

Code	Description
0	Successful completion. All records in the log file were examined successfully.
1	Invalid command-line options were specified.

#### Related Information

- [Fault Management Terminology](#)
- [View Information About Active Faulty Components \(fmadm faulty\)](#)
- [Administering Open Problems](#)

## Using `fmstat` to View the Fault Management Statistics Report

The Oracle ILOM Fault Manager maintains a viewable statistics report about diagnosis engines and agents participating in fault management operations. For more details about this report, see:

- [fmstat Report Example and Description](#)
- [View the Fault Management Statistics Report \(fmstat\)](#)

### `fmstat` Report Example and Description

- [fmstat Report Example](#)
- [fmstat Report Property Descriptions](#)

### `fmstat` Report Example

```

faultmgmtsp> fmstat
fdd statistics 2011-02-03/19:12:51

engine status evts_in evts_out errors
repair empty 8 0 0
hysteresis empty 0 0 0
SERD empty 0 0 0
simple empty 12 0 0

```

## fmstat Report Property Descriptions

Property	Description
engine	<p>The <code>engine</code> column in the <code>fmstat</code> tabular output identifies the name of the diagnosis engine:</p> <ul style="list-style-type: none"> <li><code>repair</code> – Rule that indicates a fault should be considered repaired if a specified ereport is logged. For example, the fault <code>fault.chassis.power.inadequate@/sys</code> would be considered repaired if <code>ereport.chassis.boot.power-off-requested@/system</code> was logged.</li> <li><code>hysteresis</code> – Rule to diagnose a fault if ereport <i>A</i> (initiation) is logged and ereport <i>B</i> (cancellation) is not logged within some specified time afterward. The time limit between the initiation/cancellation can be no greater than 10 seconds. For example, if <code>ereport.fan.speed-low-asserted</code> is logged and <code>ereport.fan.speed-low-deasserted</code> is logged 13 seconds later, a fault would be diagnosed.</li> <li><code>SERD</code> – Soft error rate discrimination (SERD) is used in tracking multiple occurrences of an ereport. If more than <i>N</i> ereports show up within time period <i>T</i>, the fault is diagnosed. For example, if too many correctable memory error ereports are logged within a specific time frame, a DIMM fault is diagnosed.</li> <li><code>simple</code> – Rule to allow one ereport to result in the diagnosis of multiple faults. For example, an ereport for an uncorrectable memory error can lead to a fault diagnosis for two DIMMs in a DIMM pair.</li> </ul>
status	<p>The <code>status</code> column in the <code>fmstat</code> tabular output identifies the current state of the diagnosis engine, which can include: <code>uninit</code>, <code>empty</code>, <code>enqueued</code>, <code>busy</code>, or <code>exiting</code>.</p>
evts_in	<p>The <code>evts_in</code> column in the <code>fmstat</code> tabular output identifies the number of events received by the engine that are relevant to a diagnosis.</p>
evts_out	<p>The <code>evts_out</code> column in the <code>fmstat</code> tabular output identifies the number of faults detected and posted by the engine.</p>
errors	<p>The <code>errors</code> column in the <code>fmstat</code> tabular output identifies the number of internal errors detected by the engine.</p>

View the Fault Management Statistics Report (`fmstat`)

## Before You Begin

- Review [fmstat Report Example and Description](#).

To view statistics for fault management operations from the Oracle ILOM Fault Management Shell, do the following:

1. From the Oracle ILOM CLI, launch the Fault Management Shell, as described in [Launch a Fault Management Shell Session \(CLI\)](#).

The `faultmgmtsp>` prompt appears.

2. Issue the following command to view the fault management statistics report:

```
fmstat
```

#### Related Information

- [Fault Management Terminology](#)
- [Using fmadm to Administer Active Oracle Hardware Faults](#)
- [Clearing Faults for Repairs or Replacements](#)
- [Using fmdump to View Historical Fault Management Logs](#)
- [Administering Open Problems](#)

# 9

## Using the Command-Line Interface

Description	Links
Learn about the Distributed Management Task Force command-line protocol.	<a href="#">About the Command-Line Interface (CLI)</a>
Review supported CLI syntax, commands, and options.	<a href="#">CLI Reference for Supported DMTF Syntax, Command Verbs, and Options</a>
Execute commands to change target properties.	<a href="#">CLI Reference for Executing Commands to Change Properties</a>
Learn about the CLI namespaces used for server management.	<a href="#">CLI Device Management Namespace Summary</a>
Learn about where management tasks are performed in the target namespace hierarchy.	<a href="#">CLI Reference for Mapping Management Tasks to CLI Targets</a>

### Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)

### About the Command-Line Interface (CLI)

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

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

In Oracle ILOM, the SM CLP provides a user interface for managing your servers regardless of server state, method of access, or installed operating system.

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

The SM CLP is also suitable for scripting environments. Using a scripting tool, such as Expect, you can automate testing and facilitate provisioning (such as common configuration and firmware updates) on multiple servers.

For more information about managing objects in the Oracle ILOM CLI namespace, see [Oracle ILOM CLI Namespace Targets](#).

### Related Information

- [CLI Reference for Executing Commands to Change Properties](#)
- [CLI Device Management Namespace Summary](#)
- [CLI Reference for Mapping Management Tasks to CLI Targets](#)

# CLI Reference for Supported DMTF Syntax, Command Verbs, and Options

- [Supported CLI Syntax](#)
- [Basic CLI Commands and Options](#)
- [Basic Command-Line Editing Keystrokes](#)

## Supported CLI Syntax

The supported syntax entered in the Oracle ILOM CLI to execute commands is in the form of:

```
<verb> [<-option>] [<target>] [<property>=<property_value>]
```

Where:

- **<verb>** — The term verb refers to a specific command or an action being performed. For instance, the use of a command verb enables retrieving and managing data (**set**, **show**), creating or deleting data (**create**, **delete**), modifying the state of a managed component (**set**, **reset**, **start**, **stop**), managing the current CLI session (**cd**, **version**, **exit**), as well as displaying command information (**help**).

 **Note:**

Only one command verb can be issued on a command line.

- **<-option>** — The term option refers to the command `-option` that is used to modify the action or behavior of a command verb. For instance, the use of an option can provide features for changing the CLI output format, applying a command to nested levels, or executing a script to perform one or more actions.

When entering an option on the command line, it can appear immediately after the command verb, and it must always be preceded by a hyphen (-).

 **Note:**

Not all command verbs support options. Therefore, there might be zero or more options supported for an issued command verb.

- **<target>** — The term target refers to the address or path for the issued command verb. For instance, a target can reference individual managed components (for example, a disk, a power supply, a memory module), or a collection of managed components (for example, system).

When entering a target on the command line, it can appear after the command verb but only one target can be referenced for each issued command verb.

- **<property>** — The term property is the attribute of the target that might contain values that are needed to process the command. A property identifies a target's class which is retrieved or acted upon by the command.



- `=<property_value>` — The assignment operator (=) is used to indicate a desired value to be assigned to a specified property.

## Related Information

- [Oracle ILOM CLI Supports Case Insensitive Expressions](#)

## Basic CLI Commands and Options

The Oracle ILOM CLI supports the following basic commands and options.

### Note:

The options that are enclosed in squared brackets ([]) are optional, those that are enclosed in angle brackets (<>) are keywords, and those that are separated by a pipe (|) indicate a choice of a keyword or option.

Command	Command Options	Description
cd	<code>[-default]&lt; target &gt;</code>	Navigates the target namespace. <b>-default</b> — Selects the initial default target.
create	<code>&lt; target &gt;[&lt; property &gt;=&lt; value &gt;]</code>	Creates a target and property values in the namespace (for example, to add a user and specify the user's <code>role</code> and <code>password</code> ).
delete	<code>[-script]&lt; target &gt;</code>	Removes an object from the namespace (for example, to delete a user account). <b>-script</b> — Skips warnings and prompts normally associated with the command (assumes “yes” for prompts).
dump	<code>-destination &lt; URI &gt;[-force] [&lt; target &gt;]</code>	Transfers a file from a target to a remote location specified by the URI (for example, a configuration or service snapshot). <b>-f -force</b> — Overrides internal checks and dumps the requested file. <b>-destination &lt;URI&gt;</b> — Specifies the required destination path using the uniform resource identifier (URI) format.
exit	None.	Terminates a CLI session.
help	<code>[-format wrap nowrap] [-output terse verbose]</code>	Displays Help information for commands, targets, and target properties. <b>-format wrap nowrap</b> — Specifies the screen format for Help text. <b>-o -output terse verbose</b> — Specifies the amount of Help text to be displayed.

Command	Command Options	Description
load	<code>[-output verbose] [-force] [-script] -source &lt; URI &gt;</code>	Transfers a file from an indicated source to an indicated target (for example, a configuration or firmware image). <b>-o -output verbose</b> — Specifies the amount of information text to be displayed. <b>-f -force</b> — Overrides internal checks and dumps the requested file. <b>-script</b> — Skips warnings and prompts normally associated with the command (assumes “yes” for prompts). <b>-source &lt;URI&gt;</b> — Specifies the required source path using the uniform resource identifier (URI) format.
reset	<ul style="list-style-type: none"> <li>• For X86: <code>[-script] &lt; target &gt;</code></li> <li>• For SPARC: <code>[-script] [-force] &lt; target &gt;</code></li> </ul>	Reset a target (for example, the power to a host server or to the service processor). <b>-f -force</b> — Specify the action will be performed immediately. <b>-script</b> — Skips warnings and prompts normally associated with the command (assumes “yes” for prompts).
set	<code>[&lt; target &gt;] &lt; property &gt;=&lt; value &gt; [&lt; property &gt;=&lt; value &gt;]</code>	Sets target properties to the specified value.
show	<code>[-display targets properties commands all][-a] [-level 1 2 3...255 all] [-format wrap nowrap] [-output table] [-t] [&lt; target &gt;] [&lt; property &gt; &lt; property &gt;]</code>	Displays information about targets and properties. <b>-d -display</b> — Specifies the information to be displayed. <b>-a</b> — Same as <code>-display all</code> . <b>-l -level</b> — Specifies the relative level in the target hierarchy to which the action will apply. <b>-format wrap nowrap</b> — Specifies screen format. <b>-o -output table</b> — Specifies to display the output in table format. <b>-t</b> - Same as <code>-level all -output table</code> .
start	<code>[-script] [-force] &lt; target &gt;</code>	Starts the target (for example, the host system, or an Oracle ILOM internal shell). <b>-script</b> — Skips warnings and prompts normally associated with the command (assumes “yes” for prompts). <b>-f -force</b> — Overrides internal checks and performs the action immediately.
stop	<code>[-script] [-force] &lt; target &gt;</code>	Stops the target (for example, the host system). <b>-script</b> — Skips warnings and prompts normally associated with the command (assumes “yes” for prompts). <b>-f -force</b> — Overrides internal checks and performs the action immediately.
version	None.	Displays the service processor firmware version.

## Related Information

- [Basic CLI Commands and Options](#)

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [CLI Reference for Executing Commands to Change Properties](#)
- [CLI Reference for Mapping Management Tasks to CLI Targets](#)
- [CLI Device Management Namespace Summary](#)

## Basic Command-Line Editing Keystrokes

The Oracle ILOM CLI supports the following command-line editing keystrokes:

- [Cursor Movement CLI Editing Keystrokes](#)
- [Text Deletion CLI Editing Keystrokes](#)
- [Text Input CLI Editing Keystrokes](#)
- [Command History CLI Editing Keystrokes](#)

**Table 9-1** Cursor Movement CLI Editing Keystrokes

To:	Press:
Move the cursor to the right.	<b>Right arrow</b> -or- <b>Ctrl+F</b>
Move the cursor to the left.	<b>Left arrow</b> -or- <b>Ctrl+B</b>
Move the cursor to the beginning of the command line.	<b>Ctrl+A</b>
Move the cursor to the end of the command line.	<b>Ctrl+E</b>
Move the cursor forward by one word.	<b>Esc+F</b>
Move the cursor backward by one word.	<b>Esc+B</b>

**Table 9-2** Text Deletion CLI Editing Keystrokes

To:	Press:
Delete the character before the cursor.	<b>Backspace</b> -or- <b>Ctrl+H</b>
Delete the character at the cursor.	<b>Ctrl+D</b>
Delete the characters starting from the cursor location to the end of the command line.	<b>Ctrl+K</b>
Delete the word before the cursor.	<b>Ctrl+W</b> -or- <b>Esc+H</b> -or- <b>Esc+Backspace</b>
Delete the word at the cursor.	<b>Esc+D</b>

**Table 9-3 Text Input CLI Editing Keystrokes**

To:	Press:
Complete the input of the target or property name.	<b>Tab</b>
Abort the command-line input.	<b>Ctrl+C</b>
Complete the end of multi-line input when using the commands for: <code>load -source console</code> or <code>set load_uri=console</code> .	<b>Ctrl+Z</b>

**Table 9-4 Command History CLI Editing Keystrokes**

To:	Press:
Display the command-line history.	<b>Ctrl+L</b>
Scroll backward through the command-line history.	<b>Up arrow</b> -or- <b>Ctrl+P</b>
Scroll forward through the command-line history.	<b>Down arrow</b> -or- <b>Ctrl+N</b>

## Related Information

- [Basic CLI Commands and Options](#)
- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [CLI Reference for Executing Commands to Change Properties](#)
- [CLI Reference for Mapping Management Tasks to CLI Targets](#)

# CLI Reference for Executing Commands to Change Properties

You can execute most CLI commands by specifying the command, the target, and property values to change. You can choose to execute commands that change single or multiple properties on the same command line. Some properties that can interrupt Oracle ILOM connectivity also require you to confirm the change before the change can take affect in Oracle ILOM.

For further details about executing CLI commands, see the following topics:

- [Executing Commands to Change Target Properties](#)
- [Executing Commands That Require Confirmation](#)

## Executing Commands to Change Target Properties

You can choose to execute commands to change target properties by performing any of the following methods:

- Navigating to the target, looking at its properties, and executing a command.

For example, to set the user session time-out for the Oracle ILOM web server to 30 minutes, type:

```
-> cd /SP/services/web
/SP/services/web

-> show /SP/services/web

/SP/services/web
 Targets:
 ssl

 Properties:
 allowed_services = browser, rest
 http_port = 80
 https_port = 443
 secureremote = enabled
 servicestate = enabled
 sessionduration = 1440 (24h)
 sessiontimeout = 15 (15m)
 tlsv1_2 = enabled

 Commands:
 cd
 set
 show

-> set sessiontimeout=30
```

- Entering the command and the full path to the target, from anywhere in the namespace, and changing a single property.

For example:

```
-> set /SP/services/web sessiontimeout=30
```

- Entering the command and the full path to the target, from anywhere in the namespace, and changing multiple properties.

For example:

```
-> set /SP/services/web servicestate=disable secureremote=enabled
```

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Executing Commands to Change Target Properties](#)
- [Executing Commands That Require Confirmation](#)

## Executing Commands That Require Confirmation

For targets where a change in properties can interrupt current user sessions, configuration includes committing the pending change to take affect.

For example, changing the IP network settings for the SP in Oracle ILOM will cause an interruption to the current user sessions. Therefore, you will be required to commit any changes you have made to the IP properties before your changes can take affect in Oracle ILOM.

An example of the process used to commit changes for IP properties appears below:

1. View the current network settings.

```
-> show /SP/network

/SP/network
Targets:
 interconnect
 ipv6
 test

Properties:
 commitpending = (Cannot show property)
 dhcp_clientid = none
 dhcp_server_ip = none
 ipaddress = 192.0.2.22
 ipdiscovery = static
 ipgateway = 192.0.2.1
 ipnetmask = 10.255.255.0
 macaddress = 00:28:25:E7:18:0C
 managementport = MGMT
 outofbandmacaddress = 00:28:25:E7:18:0C
 pendingipaddress = 192.0.2.22
 pendingipdiscovery = static
 pendingipgateway = 192.0.2.1
 pendingipnetmask = 10.255.255.0
 pendingmanagementport = MGMT
 sidebandmacaddress = 00:28:25:E7:18:0D
 state = enabled

Commands:
 cd
 set
 show
```

2. To change the settings, first enter the new (pending) information.

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

3. Then, after you have confirmed that the new settings are correct, commit the new settings to have them take effect immediately:

```
-> set /SP/network commitpending=true
```



**Note:**

You can also combine the commit property with the pending information in a single command.



**Note:**

If you are connecting to Oracle ILOM over a LAN, you will have to reconnect to Oracle ILOM after committing any IP property changes.

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Executing Commands to Change Target Properties](#)
- [Setting Up a Management Connection to Oracle ILOM and Logging In](#)

## CLI Device Management Namespace Summary

Oracle ILOM supports the following CLI namespaces for server management.

Server Management Namespaces	Applicable Servers and Firmware
<p>Access the service processor (SP) to 1) monitor the system health; 2) view server component inventory; and 3) configure and view Oracle ILOM administration properties.</p> <p>From the server SP CLI, you can access the following namespaces:</p> <ul style="list-style-type: none"> <li>• <code>/SP</code> – Use the <code>/SP</code> target to configure Oracle ILOM administration properties and to view log files.</li> <li>• <code>/HOST</code> – Use the <code>/HOST</code> target to monitor and manage HOST related properties.</li> <li>• <code>/Servers</code> – Use the <code>/Servers</code> target to view and manage existing PDomain configurations on multi-host SPARC servers (<code>/Servers/PDomains/PDomain_n</code> )</li> <li>• <code>/System</code> – Use the <code>/System</code> target to monitor component inventory and environmental sensors.</li> </ul>	<p>x86 servers            SPARC T and M series servers            Oracle ILOM 3.1 and later</p>



## Related Information:

- [CLI Hierarchy for Oracle ILOM 5.0.x Targets](#)
- [CLI Reference for Mapping Management Tasks to CLI Targets](#)

## CLI Reference for Mapping Management Tasks to CLI Targets

Refer to the topics in this section to help identify the applicable CLI namespace targets for the following Oracle ILOM management tasks:

- [Management Connection Tasks and Applicable CLI Targets](#)
- [Network Deployment Tasks and Applicable CLI Targets](#)
- [User Management Tasks and Applicable CLI Targets](#)
- [System Power-On Policy Tasks and Applicable CLI Targets](#)
- [System Power Usage Policy Tasks and Applicable CLI Targets](#)
- [Firmware Update Tasks and Applicable CLI Targets](#)
- [Firmware Back Up and Restore Tasks and Applicable CLI Targets](#)
- [x86 BIOS Back up and Restore Tasks and Applicable CLI Targets](#)
- [System Health Status Tasks and Applicable CLI Targets](#)
- [Event, Audit, and System Log Tasks and Applicable CLI Targets](#)
- [Alert Notification Tasks and Applicable CLI Targets](#)
- [Host Management Tasks and Applicable CLI Targets](#)
- [Remote KVMS Service State Tasks and Applicable CLI Target](#)
- [Host Serial Console Session Tasks and Applicable CLI Target](#)
- [Host Diagnostic Tasks and Applicable CLI Targets](#)
- [Fault Management Shell Session Task and Applicable CLI Target](#)
- [CLI Legacy Service State Tasks and Applicable CLI Targets](#)

## Management Connection Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM management connection tasks.

The following table does not provide the full CLI path to the `/SP` target on all managed devices. For instance, to access the `/SP` target from a multi-domain SPARC server append the applicable CLI properties to the beginning of the `/SP` target:

- SPARC multi-domain server, where applicable, append: `/Servers/PDomains/  
PDomain_n`





**Note:**

Use the **help** command to view the namespace targets supported on a server SP. For example, **help /SP/network**.

For additional information about setting up a management connection to Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Management Connection Task	CLI Properties on SP	Required User Role
View or modify the network service state property on the server SP.	/SP/network <ul style="list-style-type: none"> <li>state</li> </ul>	<ul style="list-style-type: none"> <li>Admin (a)</li> </ul>
View or modify the IPv4 network properties on the server SP.	/SP/network <ul style="list-style-type: none"> <li>ipdiscovery</li> <li>ipaddress</li> <li>ipnetmask</li> <li>ipgateway</li> <li>dhcp_clientid</li> </ul>	<ul style="list-style-type: none"> <li>Admin (a)</li> </ul>
View or modify the IPv6 network properties on the server SP.	/SP/network/ipv6 <ul style="list-style-type: none"> <li>state</li> <li>autoconfig=</li> <li>autoconfig</li> <li>static_ipaddress</li> </ul>	<ul style="list-style-type: none"> <li>Admin (a)</li> </ul>
Test IPv4 and IPv6 network connectivity.	/SP/network/ test <ul style="list-style-type: none"> <li>ping</li> </ul>	<ul style="list-style-type: none"> <li>Operator (o)</li> </ul>
View or modify the SP network management port property.	/SP/network <ul style="list-style-type: none"> <li>managementport</li> </ul> <div data-bbox="812 1260 859 1299" data-label="Image"> </div> <div data-bbox="857 1260 945 1295" data-label="Section-Header"> <p><b>Note:</b></p> </div> <div data-bbox="857 1316 1066 1463" data-label="Text"> <p>Not all server SPs support the Netn property for enabling sideband management.</p> </div>	<ul style="list-style-type: none"> <li>Admin (a)</li> </ul>

Management Connection Task	CLI Properties on SP	Required User Role
View or modify the local interconnect access properties between the Oracle ILOM SP and host OS.	/SP/network/ interconnect <ul style="list-style-type: none"> <li>• host_managed</li> </ul> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <p>Other interconnect properties can be configured if you choose to manually configure the connection between the SP and host OS. Use the <code>help</code> command to learn about the other interconnect properties.</p> </div>	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>
View or modify the Domain Name Service (DNS) resolution properties on the server SP.	/SP/clients/dns <ul style="list-style-type: none"> <li>• auto_dns</li> <li>• nameserver</li> <li>• /retries</li> <li>• searchpath</li> <li>• timeout</li> </ul>	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>
View or modify the serial management port property on the server SP.	/SP/serial <ul style="list-style-type: none"> <li>• external</li> <li>• host</li> <li>• portsharing</li> </ul> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <p>The serial port properties vary from system to system. Use the <code>help</code> command to determine which serial port properties are supported. For example: <code>help /SP/serial</code></p> </div>	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Setting Up a Management Connection to Oracle ILOM and Logging In](#)
- [Configure a Dedicated Network Management Connection to Oracle ILOM](#)
- [Configure a Sideband Management Connection to Oracle ILOM](#)
- [Manually Configure the Local Interconnect](#)

- Configure a Dedicated Local Management Connection to Oracle ILOM

## Network Deployment Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM network deployment tasks.

The following table does not provide the full CLI path to the /SP target on all managed devices. For instance, to access the /SP target from a multi-domain SPARC server append the applicable CLI properties to the beginning of the /SP target:

- SPARC multi-domain server, where applicable, append: /Servers/PDomains/  
PDomain\_n




### Note:

Use the `help` command to view the namespace targets supported on a server SP. For example, `help /SP/network/services`.

For additional information about modifying default network deployment properties in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Network Deployment Task	CLI Properties on SP	User Role Required
View or modify the network management service properties on the server SP.	/SP/services <ul style="list-style-type: none"> <li>• /web</li> <li>• /ssh               <ul style="list-style-type: none"> <li>- generate_new_key_type</li> <li>- generate_new_key_action</li> </ul> </li> <li>• /sso</li> <li>• /fips</li> <li>• /ipmi</li> <li>• /snmp</li> </ul>	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>
View or modify the CLI session time-out property on the server SP.	/SP/cli <ul style="list-style-type: none"> <li>• timeout</li> <li>• legacy_targets</li> </ul>	Admin (a)
View or terminate user sessions on server SP.	/SP/sessions	Admin (a) for Delete operations
View or set the system identification information on the server SP.	/SP <ul style="list-style-type: none"> <li>• hostname</li> <li>• system_contact</li> <li>• system_description</li> <li>• system_location</li> </ul>	Admin (a)
Create and display banner messages on the server SP.	/SP/preferences/banner <ul style="list-style-type: none"> <li>• connect</li> <li>• login</li> </ul>	Admin (a)

Network Deployment Task	CLI Properties on SP	User Role Required
View or modify the Oracle ILOM date and time properties on the server SP.	<code>/SP/clock</code> <ul style="list-style-type: none"> <li><code>datetime</code></li> <li><code>timezone</code></li> <li><code>usentpserver</code></li> </ul> <div style="border: 1px solid #0070c0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <p><code>usentpserver</code> requires the network time protocol service to be enabled (see Manage the Network Time Protocol Service in this table).</p> </div>	Admin (a)
View or set the network time protocol service property on the server SP.	<code>/SP/clients/ntp/server</code> <ul style="list-style-type: none"> <li><code>/1 address</code></li> <li><code>/2 address</code></li> </ul>	Admin (a)

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- Modifying Default Settings for Network Deployment and Administration
- Network Management Service Deployment Options
- Network Connectivity Deployment Options
- Use of Web Server Certificates and SSH Server-Side Keys
- Default Timeout for CLI and Web Sessions
- Serial Management Port Owner

## User Management Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM user management tasks.

The following table does not provide the full CLI path to the `/SP` target on all managed devices. For instance, to access the `/SP` target from a multi-domain SPARC server append the applicable CLI properties to the beginning of the `/SP` target:


- SPARC multi-domain server, where applicable, append: `/Servers/PDomains/PDomain_n`



### Note:

Use the `help` command to view the namespace targets supported on a server SP. For example, `help /SP/users`.

For additional information about setting up local or remote directory user accounts in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

User Management Task	CLI Properties on SP	User Role Required
Manage Oracle ILOM users locally (up to 10 per service processor).	/SP/users <ul style="list-style-type: none"> <li>• /username password= role=</li> </ul> Use the <b>create</b> or <b>delete</b> commands to manage local accounts. <ul style="list-style-type: none"> <li>• /set load=uri</li> </ul> Command syntax for uploading user-generated SSH Key.	<ul style="list-style-type: none"> <li>• User Management (u) to manage other users</li> <li>• Read only (o) to manage your own account</li> </ul>
Configure remote authentication directory services .	/SP/clients <ul style="list-style-type: none"> <li>• /activedirectory</li> <li>• /ldap</li> <li>• /ldapssl</li> <li>• /radius</li> </ul>	User Management (u)
Set physical presence security for Oracle ILOM default password recovery.	/SP <ul style="list-style-type: none"> <li>• check_physical_presence</li> </ul> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <p>Resetting the Oracle ILOM default password must be performed through a connection to the system's SER MGT port.</p> </div>	User Management (u)

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Setting Up and Maintaining User Accounts](#)
- [Supported User Authentication Configuration Options](#)
- [Assignable Oracle ILOM User Roles](#)
- [Single Sign-On Service \(Enabled by Default\)](#)
- [CLI Authentication Using Local User SSH Key](#)
- [Password Recovery for Default root Account](#)

## System Power-On Policy Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM SP power-on tasks.



**Note:**

Use the `help` command to view the power-on targets supported on a managed server SP. For example, type: `help /SP/policy`

For detailed information about setting the power source policies in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Power-On Policy Task	CLI Properties on SP	User Role Required
Manage system power-on policies.	<code>/SP/policy</code> <ul style="list-style-type: none"> <li>• <code>HOST_AUTO_POWER_ON</code></li> <li>• <code>HOST_LAST_POWER_STATE</code></li> <li>• <code>ENHANCED_PCIE_COOLING_MODE</code></li> </ul> <div data-bbox="787 766 833 808" data-label="Image"> </div> <div data-bbox="833 770 917 804" data-label="Section-Header"> <p><b>Note:</b></p> </div> <div data-bbox="829 825 1060 1035" data-label="Text"> <p>To determine which policy properties are supported for your device, use the <code>help</code> command (<code>help /SP/policy</code>).</p> </div>	Admin (a)

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Power-On and Cooling-Down Policies Configurable From the Server SP](#)

## System Power Usage Policy Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM system power usage policy tasks and alert notification tasks.

The following table does not provide the full CLI path to the `/SP` target on all managed devices. For instance, to access the `/SP` target from a multi-domain SPARC server append the applicable CLI properties to the beginning of the `/SP` target:

- SPARC multi-domain server, where applicable, append: `/Servers/PDomains/PDomain_n`



**Note:**

Use the `help` command to view the namespace targets supported on the managed server SP. For example, `help /SP/powermgmt`.

For detailed information about setting power usage policies and alert notifications in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Power Policy Tasks	CLI Properties on SP	User Role Required
Manage system component power from server SP. If applicable, set properties for alert notification thresholds and power budget.	/SP/powermgmt <ul style="list-style-type: none"> <li>• actual_power</li> <li>permitted_power</li> <li>allocated_power</li> <li>available_power</li> <li>• threshold1 2=</li> <li>• /powerconf</li> <li>• /budget</li> </ul>	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Setting Power Consumption Alert Notifications](#)
- [Setting SP Advanced Power Capping Policy to Enforce Power Limit](#)
- [Setting SP Advanced Power Capping Policy to Enforce Power Limit](#)
- [Set Power Management Settings for Power Policy on SPARC Servers](#)

## Firmware Update Tasks and Applicable CLI Targets

Use the following table to help identify Oracle ILOM firmware update tasks and CLI targets.

The following table does not provide the full CLI path to the /SP target on all managed devices. For instance, to access the /SP target from a multi-domain SPARC server append the applicable CLI properties to the beginning of the /SP target:

- SPARC multi-domain server, where applicable, append: /Servers/PDomains/PDomain\_n






### Note:

Use the `help` command to view the namespace targets supported on a server SP. For example, `help /SP/Firmware`.

For detailed information about how to perform Oracle ILOM firmware updates, see the topics listed in the Related Information section that appears after the table.



Firmware Tasks	CLI Properties on SP	User Role Required
View system BIOS properties or update system BIOS image (x86 only).	/System/BIOS <ul style="list-style-type: none"> <li>• system_bios_version</li> <li>• boot_mode</li> </ul> <div style="border: 1px solid #0070c0; padding: 5px; margin: 10px 0;">  <b>Note:</b>              To change the BIOS boot mode, refer to the administration guide provided for the server.           </div> <ul style="list-style-type: none"> <li>• reset_to_defaults</li> <li>• /Config load_uri</li> </ul>	<ul style="list-style-type: none"> <li>• Read only (o)</li> <li>• Admin (a) for loading new image.</li> </ul>
View the Oracle ILOM firmware version installed.	/System/Firmware <ul style="list-style-type: none"> <li>• system_fw_version</li> </ul>	<ul style="list-style-type: none"> <li>• Read only (o)</li> </ul>
Update the SP firmware image.	/SP/Firmware <ul style="list-style-type: none"> <li>• load_uri</li> <li>• /host/miniroot</li> <li>• /keys</li> <li>• /backupimage</li> </ul> <div style="border: 1px solid #0070c0; padding: 5px; margin: 10px 0;">  <b>Note:</b>              To view which firmware properties are supported, use the help command (help /SP/ firmware)           </div> <div style="border: 1px solid #0070c0; padding: 5px; margin: 10px 0;">  <b>Note:</b>              SPARC server platforms require the host operating system to be powered-off prior to performing the firmware update.           </div>	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Updating Oracle ILOM Firmware](#)
- [Firmware Upgradable Devices](#)

## Firmware Back Up and Restore Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace target for Oracle ILOM back up or restore configuration tasks or to reset the Oracle ILOM configuration to factory defaults.

The following table does not provide the full CLI path to the /SP target on all managed devices. For instance, to access the /SP target from a multi-domain SPARC server append the applicable CLI properties to the beginning of the /SP target:

- SPARC multi-domain server, where applicable, append: /Servers/PDomains/  
PDomain\_n



### Note:

Use the **help** command to view the namespace targets supported on a server SP. For example, **help /SP/Config**.

For detailed information about backing up or restoring the SP configuration in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

Firmware Backup and Restore Tasks	CLI Properties on SP	User Role Required
Back up or restore Oracle ILOM SP configurations.	/SP/Config <ul style="list-style-type: none"> <li>• dump_uri Backs up configuration to xml file.</li> <li>• load_uri Restores configuration from xml file.</li> </ul>	<ul style="list-style-type: none"> <li>• Admin (a)</li> <li>• User Management (u)</li> <li>• Console (c)</li> <li>• Reset and HostControl (r)</li> <li>• Read Only (o)</li> </ul>
Reset Oracle ILOM configuration properties to defaults upon next SP reboot.	/SP reset_to_defaults = <ul style="list-style-type: none"> <li>• all Resets all properties.</li> <li>• factory Resets all properties and erases log data.</li> <li>• none Cancels the reset operation; must be done before next reboot.</li> </ul>	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- Backing Up, Restoring, or Resetting the Oracle ILOM Configuration
- Password Recovery for Default root Account

## x86 BIOS Back up and Restore Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM x86 BIOS configuration tasks.

For detailed information about backing up or restoring the x86 BIOS configuration in Oracle ILOM, see the topics listed in the Related Information section that appears after the table.

BIOS Management Tasks	CLI Properties on SP	User Role Required
Back up or restore the system BIOS configuration from an x86 server SP.	/System/BIOS/ Config	<ul style="list-style-type: none"> <li>Admin (a) for save or restore</li> <li>Reset and Host Control (r) for restore</li> </ul>
Reset system BIOS configurations to factory defaults from an x86 server SP.	/System/BIOS <ul style="list-style-type: none"> <li>reset_to_defaults</li> </ul>	<ul style="list-style-type: none"> <li>Admin (a) for save or restore</li> <li>Reset and Host Control (r) for restore</li> </ul>
If applicable, modify BIOS boot mode from an x86 server SP.	/System/BIOS <ul style="list-style-type: none"> <li>boot_mode</li> </ul>	Admin (a)

### Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- Maintaining x86 BIOS Configuration Parameters
- Requirements for BIOS Configuration Tasks

## System Health Status Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI targets for Oracle ILOM system and component-level health status tasks.

For detailed information about monitoring system health in Oracle ILOM, see the topic listed in the Related Information section that appears after the table.

Health Status Tasks	CLI Properties on SP	User Role Required
View system details from a server SP.	/System/ <ul style="list-style-type: none"> <li>Open_Problems</li> <li>Processors</li> <li>Memory</li> <li>Power</li> <li>Cooling</li> <li>Storage</li> <li>Networking</li> <li>PCI_Devices</li> <li>Firmware</li> <li>BIOS</li> <li>IO_Modules</li> </ul>	<ul style="list-style-type: none"> <li>Read only (o)</li> </ul>

Health Status Tasks	CLI Properties on SP	User Role Required
View system details from a SPARC multi-domain SPARC server.	/System/ <ul style="list-style-type: none"> <li>• Open_Problems</li> <li>• DCUs</li> <li>• Processors</li> <li>• Memory</li> <li>• Power</li> <li>• Cooling</li> <li>• Log</li> </ul>	<ul style="list-style-type: none"> <li>• Read only (o) to view</li> </ul>

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Viewing System Inventory, Health, and Performing Service and Management Actions](#)

## Event, Audit, and System Log Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for managing log entries in Oracle ILOM.

For detailed information about managing Oracle ILOM logs, see the log management topic listed in the Related Information section that appears after this table.

Log Management Tasks	CLI Properties on Server SP	User Role Required
View, filter, or clear entries in the audit log or event log.	/SP/logs/ <ul style="list-style-type: none"> <li>• audit</li> <li>• event</li> </ul> <p><b>For a list of filter property values, click the <i>More details...</i> link on the Administration &gt; Logs page in the Oracle ILOM web interface.</b></p>	<ul style="list-style-type: none"> <li>• Read only (o) to view</li> <li>• Admin (a) to clear</li> </ul>
View or clear system log entries..	/System/Log	<ul style="list-style-type: none"> <li>• Read only (o) to view</li> <li>• Admin (a) to clear</li> </ul>
Set up log centralization by using a syslog server. Set the address or domain name of the primary and secondary syslog servers that will maintain a copy of the Oracle ILOM logs.	/SP/clients/syslog	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>

## Related Information

- [Managing Oracle ILOM Log Entries](#)
- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)

## Alert Notification Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for managing Oracle ILOM alert notification rules.

For detailed information about how to set alert notifications in Oracle ILOM, see the topics listed in the Related Information section after this table.

Alert Notification Tasks	CLI Properties on SP	User Role Required
Manage up to 15 alert notification rules. Set the alert type, level, and port destination for each rule.	<code>/SP /alertmgmt/ rules</code> SNMP and IPMI services must be enabled to process SNMP and IPMI alert notifications. Both of these services are enabled by default. The SMTP server must be enabled to process email alert notifications.	<ul style="list-style-type: none"> <li>Admin (a)</li> </ul>
Configure an SMTP server for email alerts.. Enable email alerts by setting an IP or DNS host name.	<code>/SP/clients/smt</code>	<ul style="list-style-type: none"> <li>Admin (a)</li> </ul>

### Related Information

- [Configure SMTP Client for Email Alerts](#)
- [Setting Power Alert Notifications and Managing System Power Usage](#)
- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)

## Host Management Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI targets for performing host management tasks on a managed server.

For additional information about how to perform host management actions in Oracle ILOM, see the topic listed in the Related Information section that appears after the table.

Host Management Tasks	CLI Properties on SP	User Role Required
Power on (start) or power off (stop) the server SP.	<code>/System</code>	<ul style="list-style-type: none"> <li>Reset and Host Control (r)</li> </ul>
Reset power on a server SP.	<code>/SP</code>	<ul style="list-style-type: none"> <li>Reset and Host Control (r)</li> </ul>
Turn on or turn off the system Locator LED.	<code>/System/locator_indicator</code>	<ul style="list-style-type: none"> <li>Admin (a)</li> </ul>
Set the boot device for the next host boot from an x86 server SP.	<code>/HOST/boot_device</code> To issue the full boot device path from the FMM CLI, append <code>/Servers/ComputeNodes/ComputeNode_n</code> to the beginning of the <code>/HOST/boot_device</code> target.	<ul style="list-style-type: none"> <li>Reset and Host Control (r)</li> </ul>

Host Management Tasks	CLI Properties on SP	User Role Required
<p>Manage the domain boot device from a SPARC server SP.</p> <p>Set auto boot for both the host controller and guest domains at startup.</p> <p>Set boot guests to enable or disable guest domain booting at startup.</p>	<p>/HOST/domain/</p> <ul style="list-style-type: none"> <li>configs</li> <li>control</li> </ul> <p>To issue the full CLI path for host domain on a multi-domain SPARC server, append /Servers/PDomains/PDomain_n to the beginning of the /HOST target.</p>	<ul style="list-style-type: none"> <li>Reset and Host Control (r)</li> </ul>
<p>Set the host boot method properties on SPARC servers.</p>	<p>/HOST</p> <ul style="list-style-type: none"> <li>autostart</li> <li>autorunonerror</li> <li>bootfailrecovery</li> <li>bootrestart</li> <li>boottimeout</li> <li>maxbootfail</li> </ul> <p>To issue the full CLI path for boot method on a multi-domain SPARC server, append /Servers/PDomains/PDomain_n to the beginning of the /HOST target.</p>	<ul style="list-style-type: none"> <li>Reset and Host Control (r)</li> </ul>
<p>Set the trusted platform module (TPM) device on a SPARC server.</p>	<p>/HOST/tpm</p> <ul style="list-style-type: none"> <li>activate</li> <li>enable</li> <li>forceclear</li> <li>mode</li> </ul> <p>TPM properties vary from system to system. Use the Help command to determine which TPM properties are supported on your server. For example: help /HOST/tpm</p> <p>To issue the full CLI path for host TPM on a multi-domain SPARC server, append /Servers/PDomains/PDomain_n to the beginning of the /HOST/tpm target.</p>	<ul style="list-style-type: none"> <li>Reset and Host Control (r)</li> </ul>

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Configuring Host Server Management Actions](#)

## Remote KVMS Service State Tasks and Applicable CLI Target

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM KVMS tasks.

For detailed information about configuring the KVMS service in Oracle ILOM, see the topic listed in the Related Information section that appears after the table.

Remote KVMS Tasks	CLI Properties on SP	User Role Required
Configure the SP remote KVMS service.	<p>/SP/services/kvms</p> <ul style="list-style-type: none"> <li>• servicestate</li> <li>• mousemode</li> <li>• display_quality</li> <li>• lockmode</li> <li>• custom_lock_key</li> <li>• custom_lock_modifiers</li> </ul> <p>To issue the full CLI path for KVMS services from a multi-domain SPARC server, append /Servers/PDomains/PDomain_n to the beginning of the /SP/services/kvms target.</p>	Admin (a)

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Using Remote KVMS Consoles for Host Server Redirection](#)

## Host Serial Console Session Tasks and Applicable CLI Target

Use the following table to help identify the applicable CLI namespace targets for starting or ending a host serial console session.



### Note:

This feature is for text-only serial console redirection. For remote graphical console redirection from Oracle ILOM, use the applicable remote system console (Oracle ILOM Remote System Console or Oracle ILOM Remote System Console Plus).

Host Serial Console Tasks	CLI Properties on SP	User Role Required
View, start, or stop a remote serial host console session.	<p>/HOST/console</p> <ul style="list-style-type: none"> <li>• bootlog</li> <li>• history</li> <li>• start</li> <li>• stop</li> <li>• show</li> </ul> <p>Host console properties vary from system to system. Use the <code>Help</code> command to determine which host console properties are supported on your server. For example:  <code>help /HOST/console</code></p> <p>To issue the full CLI path for host console from a multi-domain SPARC server, append /Servers/PDomains/PDomain_n to the beginning of the /HOST/console target.</p>	<ul style="list-style-type: none"> <li>• Console (c)</li> </ul>

## Related Information

- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)
- [Establishing a Host Serial Console Session to the Server \(CLI\)](#)

## Host Diagnostic Tasks and Applicable CLI Targets

Use the following table to help identify the applicable CLI namespace targets for Oracle ILOM host diagnostic tasks.

For detailed information about host diagnostics, see the topics listed in the Related Information section that appears after the table.

Host Diagnostic Tasks	CLI Properties on SP	User Role Required
View or modify host diagnostic properties on an x86 server.	/HOST/diag state <ul style="list-style-type: none"> <li>• enabled</li> <li>• disabled</li> <li>• extended</li> <li>• manual</li> <li>• set</li> </ul> To run and view diagnostics, launch the remote system console from the web interface, and then restart the server.	<ul style="list-style-type: none"> <li>• Reset and Host Control (r)</li> </ul>
View or modify host diagnostic properties on a SPARC server.	/HOST/diag <ul style="list-style-type: none"> <li>• error_reset_level</li> <li>• error_reset_verbosity</li> <li>• hw_change_level</li> <li>• hw_change_verbosity</li> <li>• level</li> <li>• max</li> <li>• power_on_level</li> <li>• power_on_verbosity</li> <li>• trigger</li> <li>• verbosity</li> <li>• set</li> </ul> SPARC host diagnostic properties vary from system to system. Use the <code>Help</code> command to determine which host diag properties are supported on your server. For example: <code>help /HOST/diag</code>  To issue the full CLI path for host diag from a multi-domain SPARC server, append <code>/Servers/PDomains/PDomain_n</code> to the beginning of the <code>/HOST/diag</code> target.  To run and view diagnostics, launch the remote system console from the web interface, and then restart the system.	<ul style="list-style-type: none"> <li>• Reset and Host Control (r)</li> </ul>



Host Diagnostic Tasks	CLI Properties on SP	User Role Required
View or modify SP diagnostic properties on M7 or T7 series SPARC servers.	/SP/diag <ul style="list-style-type: none"> <li>• default_level</li> <li>• hw_change_level</li> </ul> To run and view diagnostics, launch the remote console from the web interface, and then restart the system.	<ul style="list-style-type: none"> <li>• Reset and Host Control (r)</li> </ul>

## Related Information

- [Setting Diagnostic Tests to Run](#)
- [Troubleshooting Oracle ILOM Managed Devices](#)
- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)

## Fault Management Shell Session Task and Applicable CLI Target

Use the following table to help identify the CLI namespace target for the Oracle ILOM Fault Management Shell. This table does not provide the full CLI path to the /SP target on all managed devices. For instance, to access the /SP target from a multi-domain SPARC server append the applicable CLI properties to the beginning of the /SP target:

- SPARC multi-domain server, where applicable, append: /Servers/PDomains/  
PDomain\_n

All component faults reported in Oracle ILOM are automatically cleared upon the service repair or replacement of the component. For detailed information about the Oracle ILOM Fault Management Shell or the open problems reported in Oracle ILOM, see the topics in the Related Information section that appears after the following table.



### Note:

The purpose of the Oracle ILOM Fault Management Shell is to help Oracle Services personnel diagnose system problems. Customers should not run commands in the shell unless requested to do so by Oracle Services.

Fault Management Task	CLI Properties on SP	User Role Required
Launch the Fault Management shell to diagnose system problems on a server SP (as instructed by Oracle Service).	/SP/faultmgmt/shell	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>

## Related Information

- [Managing Oracle Hardware Faults Through the Oracle ILOM Fault Management Shell](#)
- [Administering Open Problems](#)
- [Navigating the Command-Line Interface \(CLI\) Namespace Targets](#)

## CLI Legacy Service State Tasks and Applicable CLI Targets

Use the following table to help identify the legacy Oracle ILOM 3.0 CLI namespace targets.

CLI Legacy Tasks	CLI Properties on SP	User Role Required
Show legacy CLI targets on server SP.	/SP/cli <ul style="list-style-type: none"> <li>• legacy_targets</li> </ul> The /SYS and /STORAGE targets are similar to /System targets. Refer to the Oracle ILOM 3.0 documentation for details.	<ul style="list-style-type: none"> <li>• Admin (a)</li> </ul>

# 10

## 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 consumption

The amount of power wattage used by the server.

#### 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).

## allocated power

The maximum input power wattage assigned to a managed device.

## audit log

A log that tracks all interface-related user actions, such as user logins, logouts, configuration changes, and password changes. The user interfaces monitored for user actions include: Oracle ILOM web interface, CLI, Fault Management Shell (captive shell), Restricted Shell, as well as SNMP and IPMI client interfaces.

## 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.

## 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.

### 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.

### Common Information Model (CIM)

The Common Information Model (CIM) is a computer industry standard for defining device and application characteristics so that system administrators and management programs can control devices and applications from different manufacturers or sources in the same way.

### 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 that 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.

## event log

A log that tracks informational, warning, or error messages about a managed device, such as the addition or removal of a component or the failure of a component. The properties of the events recorded in the log can include: the severity of the event, the event provider (class), and the date and time the event was logged.

## exhaust temperature

The temperature of air exiting the back of the server or chassis.

## 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 so a user can reach the console prompt. The 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

A detected error condition in the hardware or software.

## Fault Management Architecture (FMA)

An architecture that ensures that a computer can continue to function despite a hardware or software failure.

## Fault Manager

An Oracle ILOM feature that enables you to proactively monitor the health of your system hardware, as well as diagnose hardware failures as they occur. When a component is in a faulty state, fault events are captured in the Oracle ILOM Open Problems table and the event log.

## Fault Manager shell

A user interface that enables Oracle Services personnel to diagnose system problems. Users can run commands in this shell only if requested to do so by Oracle Services.

### faulted state

An indicator of a component that is present but is unusable or degraded because one or more problems have been diagnosed by Oracle ILOM. Oracle ILOM automatically disables the component to prevent further damage to the system.

## 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 the 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

### health status states

Indicators that specify the health of the managed device. Possible status states are: OK, Service Required, Not Available, and Offline.

### 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.

---

## in-band system management

Server management capability that is enabled only when the operating system is initialized and the server is functioning properly.

## inlet air temperature

The temperature entering into the front of the server or chassis.

## installed hardware minimum

The smallest amount of input power wattage consumed by the hardware components installed on the server.

## 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-replaceable unit (FRU) inventory reporting, system monitoring, logging, system recovery (including local and remote system resets and power-on and power-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 “192.0.2.1” which specifies the actual location of a machine on an intranet or the Internet.

## input power

Power that is pulled into the chassis power supply units from an external power source.

## 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 Web Start application

A web application launcher. With Java Web Start, you launch applications by clicking 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 through 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.

## maximum permitted power

See peak permitted.

## 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.

## notification threshold

A value that defines the amount of power wattage consumed that will trigger an alert notification.

## 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 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).

## open problem

An indicator that a problem, or fault condition, is detected on a managed device. Oracle ILOM identifies the problem on the Open Problems web page or the Open Problems tabular CLI output.

## Operator

A user with limited privileges to the managed host system.

## Oracle ILOM Remote System Console (Plus)

A graphical remote console feature that enables users to redirect devices (keyboard, mouse, video display, storage media) from a desktop to a remote host server.

## out-of-band (OOB) system management

Server management capability that is enabled when the operating system network drivers or the server is not functioning properly.

## output power

The amount of power provided from the power supply units to the chassis components.

## 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.

## peak permitted

The maximum power wattage a managed device can consume.

## 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 consumption

The maximum power wattage that the server is permitted to use 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 allocation plan

A feature that enables a user to effectively monitor and acquire the precise power metrics allocated to a single managed device, or to the individual components installed on a managed device. This aids in planning an energy-efficient data center.

## power consumption

A value that shows either the input power consumed by the managed device or the output power provided by the power supply units (PSUs).

## power cycling

The process of turning the power to a system off then on again.

## power supply maximum

The largest amount of input power wattage that the power supplies are capable of consuming.

## 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 second 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)

A standard for Internet electronic mail that encrypts data to ensure privacy and data integrity.

## protocol

A set of rules that describes how systems or devices on a network exchange information.

## proxy

A mechanism whereby one system acts on behalf of another system in responding to protocol requests.

## public key encryption

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

### rackmount server power consumption

The sum of input power being consumed by the rackmount chassis power supplies.

### real-time clock (RTC)

A battery-backed component that maintains the time and date for a system, even when the system is powered off.

### real-time power monitoring

A feature that, through polling hardware interfaces, provides continuously updated power consumption metrics, within one second of accuracy.

### 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.

## S

## 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.

## 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 Sockets 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

An identifiably separate part of an organization's network. A subnet can divide 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."

## 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 log

The top-level system log presents a subset of relevant operational Event Log entries. Specifically, this log reports subsystem level diagnostic events pertaining to system inventory actions and component health. These events can include power on and off, FRU insertion and removal, as well as health status events, such as service required, warning, or OK.

## 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

## target

In the Oracle ILOM command-line interface, every object in the CLI namespace.

## target limit

A value, set on the Oracle server, that determines (by wattage or percentage) the power budgeting parameters allowed on the server.

## target namespace

In the Oracle ILOM command-line interface, a hierarchical, predefined tree that contains every managed object in the system. For more details, see [namespace](#).

## 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 Oracle 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, through 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

## C

---

command-line interface  
target tree, [10-23](#)

## O

---

Oracle Integrated Lights Out Manager (ILOM)  
performing common management actions  
(web), [4-16](#)

## V

---

viewing  
subcomponent-level information (web), [4-2](#)