

**Oracle® ILOM Administrator's Guide for
Configuration and Maintenance Firmware
Release 4.0.x**



Part No: E86149-08
July 2020

Part No: E86149-08

Copyright © 2018, 2019, Oracle and/or its affiliates.

License Restrictions Warranty/Consequential Damages Disclaimer

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.

Warranty Disclaimer

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.

Restricted Rights Notice

If this is software 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" or "commercial computer software documentation" 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.

Hazardous Applications Notice

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.

Trademark Notice

Oracle and Java 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.

Third-Party Content, Products, and Services Disclaimer

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.

Pre-General Availability Draft Label and Publication Date

Pre-General Availability: 2020-01-15

Pre-General Availability Draft Documentation Notice

If this document is in public or private pre-General Availability status:

This documentation is in pre-General Availability status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

Oracle Confidential Label

ORACLE CONFIDENTIAL. For authorized use only. Do not distribute to third parties.

Revenue Recognition Notice

If this document is in private pre-General Availability status:

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your pre-General Availability trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Référence: E86149-08

Copyright © 2018, 2019, Oracle et/ou ses affiliés.

Restrictions de licence/Avis d'exclusion de responsabilité en cas de dommage indirect et/ou consécutif

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

Exonération de garantie

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

Avis sur la limitation des droits

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

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" or "commercial computer software documentation" 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.

Avis sur les applications dangereuses

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

Marques

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

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

Avis d'exclusion de responsabilité concernant les services, produits et contenu tiers

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

Date de publication et mention de la version préliminaire de Disponibilité Générale ("Pre-GA")

Version préliminaire de Disponibilité Générale ("Pre-GA") : 15.01.2020

Avis sur la version préliminaire de Disponibilité Générale ("Pre-GA") de la documentation

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère public ou privé :

Cette documentation est fournie dans la Version préliminaire de Disponibilité Générale ("Pre-GA") et uniquement à des fins de démonstration et d'usage à titre préliminaire de la version finale. Celle-ci n'est pas toujours spécifique du matériel informatique sur lequel vous utilisez ce logiciel. Oracle Corporation et ses affiliés déclinent expressément toute responsabilité ou garantie expresse quant au contenu de cette documentation. Oracle Corporation et ses affiliés ne sauraient en aucun cas être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'utilisation de cette documentation.

Mention sur les informations confidentielles Oracle

INFORMATIONS CONFIDENTIELLES ORACLE. Destinées uniquement à un usage autorisé. Ne pas distribuer à des tiers.

Avis sur la reconnaissance du revenu

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère privé :

Les informations contenues dans ce document sont fournies à titre informatif uniquement et doivent être prises en compte en votre qualité de membre du customer advisory board ou conformément à votre contrat d'essai de Version préliminaire de Disponibilité Générale ("Pre-GA") uniquement. Ce document ne constitue en aucun cas un engagement à fournir des composants, du code ou des fonctionnalités et ne doit pas être retenu comme base d'une quelconque décision d'achat. Le développement, la commercialisation et la mise à disposition des fonctions ou fonctionnalités décrites restent à la seule discrétion d'Oracle.

Ce document contient des informations qui sont la propriété exclusive d'Oracle, qu'il s'agisse de la version électronique ou imprimée. Votre accès à ce contenu confidentiel et son utilisation sont soumis aux termes de vos contrats, Contrat-Cadre Oracle (OMA), Contrat de Licence et de Services Oracle (OLSA), Contrat Réseau Partenaires Oracle (OPN), contrat de distribution Oracle ou de tout autre contrat de licence en vigueur que vous avez signé et que vous vous engagez à respecter. Ce document et son contenu ne peuvent en aucun cas être communiqués, copiés, reproduits ou distribués à une personne extérieure à Oracle sans le consentement écrit d'Oracle. Ce document ne fait pas partie de votre contrat de licence. Par ailleurs, il ne peut être intégré à aucun accord contractuel avec Oracle ou ses filiales ou ses affiliés.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité de la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse : <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

Contents

Using This Documentation	15
Setting Up a Management Connection to Oracle ILOM and Logging In	17
Establishing a Management Connection to Oracle ILOM	17
Choosing and Configuring a Management Connection to Oracle ILOM	18
Management Services and Network Default Properties	33
Logging In to Oracle ILOM Server SP or CMM	35
▼ Log In to the Oracle ILOM SP or CMM	36
Usage Guidelines for IP Network Management Address	37
Preconfigured User Accounts Enabled by Default	38
Supported Web Browsers for Oracle ILOM	40
Configuring Oracle ILOM for Increased Security	40
Setting Up and Maintaining User Accounts	41
Managing User Credentials	41
Supported User Authentication Configuration Options	42
Assignable Oracle ILOM User Roles	43
Single Sign-On Service (Enabled by Default)	45
Maximum Number of User Sessions Supported	46
Manage User Authenticated Sessions per Managed Device	46
CLI Authentication Using Local User SSH Key	48
Security Action: Change Default root Account Password	49
Password Recovery for Default root Account	49
Supported File Transfer Methods	50
Configuring Local User Accounts	51
Managing Password Policy Restrictions for Local Users	53
▼ Modify Password Policy Restrictions for Local Users	54
Password Policy Management Properties and Defaults	57

Configuring Active Directory	59
Configuring LDAP/SSL	69
Configuring LDAP	79
Configuring RADIUS	82
Modifying Default Settings for Network Deployment and Administration	85
Network Deployment Principles and Considerations	85
Network Management Service Deployment Options	86
Network Connectivity Deployment Options	88
Operating Oracle ILOM in FIPS Compliance Mode	89
Management of SSH Server State and Weak Ciphers	93
Use of Web Server Certificates and SSH Server-Side Keys	93
Default Timeout for CLI and Web Sessions	93
Management of Banner Messages at Log-In	94
Input Format for IPv4 and IPv6 Addresses	98
Serial Management Port Owner	98
Default Network Ports Used by Oracle ILOM	99
Legacy Oracle Servers Not Supporting IPv6	100
Modifying Default Management Access Configuration Properties	100
Modifying Default Connectivity Configuration Properties	118
Example Setup of Dynamic DNS	137
▼ Example: Set Up DDNS Configuration	137
Assigning System Identification Information	140
Setting ILOM Clock Properties	142
Suggested Resolutions for Network Connectivity Issues	143
Resolving Connectivity Issues	144
Recommended Practice for Spanning Tree Configurations	145
▼ Test IPv4 and IPv6 Connectivity	145
Using Remote KVMS Consoles for Host Server Redirection	147
Oracle ILOM Remote KVMS Consoles Supported	148
Establishing a Host Serial Console Session to the Server (CLI)	149
▼ Start Serial Console Redirection and Log In to Host Server OS	149
▼ Dump Full Console History Contents to Remote Location	151
Host Serial Console Log Properties	152
Redirecting an Image File From a Storage Device to the Host Server	155
Special Considerations for Configuring Host Storage Device Properties	156

CLI and Web Host Storage Device Properties	157
▼ Uploading a New Solaris Miniroot Package From SP to Host	160
System Management Miniroot Property Descriptions	162
Connecting to the Oracle ILOM Remote System VNC Console	163
Before You Begin	163
▼ Establishing an Oracle ILOM Remote System VNC Console Connection	165
Troubleshooting the VNC Connection	166

Using the Oracle ILOM Remote System Console or Storage Redirection

CLI	167
Oracle ILOM Remote System Console	168
Remote System Console First-Time Setup	168
Requirements for Using the Oracle ILOM Remote System Console	169
▼ Configure Local Client KVMs Settings	170
▼ Register 32-Bit JDK Java Plug-In For Windows IE Web Browser	172
▼ Register 32-Bit JDK Java Plug-In for Mozilla Firefox Web Browser	172
Optionally Set a Lock Mode to Secure the Host Server Desktop	173
Launching and Using the Oracle ILOM Remote System Console	176
▼ Launch and Use the Oracle ILOM Remote System Console	176
Remote System Console Menu Options, Usage Considerations, and Toggle Keys	178
Redirection Menu Options	178
Devices Menu Options	179
Device Redirection Usage Considerations	179
Keyboard Menu Options	180
Toggle Key Sequence for Keyboard and Mouse Control	181
International Keyboard Support	181
Oracle ILOM Storage Redirection CLI	181
Storage Redirection CLI First-Time Setup	181
Requirements for Using the Oracle ILOM Storage Redirection CLI	182
▼ Register Java Plug-In for Windows IE Browser and Start Service for First Time	183
▼ Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser	184
▼ Install the Storage Redirection Client	185
▼ Optionally Modify the Default Network Port 2121 for Storage Redirection	186
Launching and Using the Oracle ILOM Storage Redirection CLI	188

▼ Launch the Oracle ILOM Storage Redirection CLI and Redirect Storage Devices	188
Interactive and Non-Interactive Shell Syntax	192
Storage Redirection Commands and Options	192
Using the Oracle ILOM Remote System Console Plus	197
Oracle ILOM Remote System Console Plus	198
Remote System Console Plus First-Time Setup	199
Requirements for Using the Oracle ILOM Remote System Console Plus	200
▼ Configure Local Client KVMs Settings	202
▼ Modify KVMs Maximum Client Session Count (Optional)	204
Set a Lock Mode to Secure the Host Server Desktop (Optional)	205
Launching and Using the Oracle ILOM Remote System Console Plus	207
▼ Launch and Use the Oracle ILOM Remote System Console Plus	208
Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards	212
KVMs Menu Options	212
Preference Menu Options	214
Help Menu Options	215
International Keyboard Support	215
Toggle Button, Virtual Keys, and Status Icons	215
Resolving Warning Messages for Self-Signed SSL Certificate	216
Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate	218
Configuring Host Server Management Actions	221
Controlling Host Power to Server or Blade System Chassis	222
Setting Diagnostic Tests to Run	223
Setting Next Boot Device on x86 Host Server	230
Setting Host Control and Boot Properties on SPARC Host Server	233
Overriding SPARC Host Boot Mode	238
Configuring SPARC Verified Boot Properties	240
Managing SPARC Host Domains	242
Setting SPARC Host KeySwitch State	244
Setting SPARC Host TPM State	245
Setting SPARC Host State Capture	248
Managing SPARC Host I/O Reconfiguration Policy	250

Managing SPARC PDomains and DCU Assignments	251
Host-DCU Assignments and DCU-SPP Failover Behavior	251
PDomain and DCU Assignments	255
Redirecting Host Output to Rear VGA Port	259
Configuring Alert Notifications, Service Requests, or Remote Logging	261
Configuring Alert Notifications	261
Alert Notification Configuration Properties	262
▼ Configure and Test Alert Notification (IPMI PET, SNMP, or Email)	264
▼ Disable Alert Notification (IPMI PET, SNMP, or Email)	265
▼ Configure SMTP Client for Email Alerts	266
Managing Automatic Service Requests	267
▼ Configure Oracle ILOM as an ASR Client	267
▼ Manage Endpoint SSL Certificate Information	268
▼ Send an ASR Test or Heartbeat Message	269
ASR Configuration Properties	270
Configuring Syslog for Event Logging	272
▼ Configure Syslog IP Address for Event Logging	273
Setting System Management Power Source Policies and Device	
Monitoring	275
Power-On and Cooling-Down Policies Configurable From the Server SP	275
System Management Power Supply Policies Configurable From CMM	278
Setting Device Monitoring Configuration Properties	280
Setting Power Alert Notifications and Managing System Power Usage	283
Setting Power Consumption Alert Notifications	283
Setting CMM Power Grant and SP Power Limit Properties	284
▼ Set CMM Blade Slot Grant Limit Property	285
▼ Set SP Power Target Limit Properties	286
Setting SP Advanced Power Capping Policy to Enforce Power Limit	287
▼ Set Advanced Power Capping Policy	288
Setting SP Power Management Settings for Power Policy (SPARC)	289
▼ Set Power Management Settings for Power Policy on SPARC Servers	290
Setting the CMM Power Supply Redundancy Policy	291
▼ Set CMM Power Supply Redundancy Policy	291

Performing Oracle ILOM Maintenance and Configuration Management Tasks	293
Updating Oracle ILOM Firmware	293
Firmware Upgradable Devices	294
Preserve Oracle ILOM Configuration	294
Before You Begin the Firmware Update	295
▼ Update the Server SP or CMM Firmware Image	296
▼ Update Blade Chassis Component Firmware Images	298
▼ Recover From a Network Failure During Firmware Update	301
Reset Power to Service Processor or Chassis Monitoring Module	301
▼ Reset Power to Server SP, NEM SP, or CMM	302
Managing ASR Component States	303
▼ Manually Enable or Disable an ASR Component	303
Managing Active and Standby SP Redundancy Roles (SPARC)	304
▼ Modify Active and Standby SP Redundancy Roles (SPARC)	305
SP Redundancy Status Descriptions	306
Backing Up, Restoring, or Resetting the Oracle ILOM Configuration	306
Using Backup, Restore, and Reset Default Operations	307
User Role Required for Backing Up or Restoring the Oracle ILOM Configuration	308
▼ Back Up the Oracle ILOM Configuration Settings	308
▼ Optionally Edit the Oracle ILOM Backup XML Configuration File	310
▼ Restore the Oracle ILOM Backup XML File	313
▼ Reset the Oracle ILOM Configuration to Factory Defaults	315
 Maintaining x86 BIOS Configuration Parameters	317
BIOS Configuration Management	317
Oracle ILOM: BIOS Configuration Features	318
Oracle ILOM: BIOS Special Considerations	318
Oracle ILOM: BIOS Terminology	319
Web and CLI: BIOS Properties	319
Performing BIOS Configuration Tasks From Oracle ILOM	323
Requirements for BIOS Configuration Tasks	323
▼ View the BIOS Configuration Sync Status and Sync the Configuration Parameters	324
▼ Reset BIOS Configuration to Factory Defaults	325
▼ Reset Factory Defaults for SP and Oracle ILOM BIOS	326

▼ Back Up the BIOS Configuration	327
▼ Restore BIOS Configuration	328
SAS Zoning Chassis Blade Storage Resources	331
Zone Management for Chassis-Level SAS-2 Capable Resources	331
Zone Management Using a Third-Party In-Band Management Application	332
Zone Management Using Oracle ILOM Sun Blade Zone Manager	332
Manageable SAS-2 Zoning-Capable Devices	332
Sun Blade Zone Manager Properties	333
Sun Blade Zone Manager Web: Properties	333
Zoning Reset: Reset All	339
Sun Blade Zone Manager CLI: Targets and Properties	340
Important SAS Zoning Allocations Considerations	341
Saving Storage Allocations	342
Backing Up and Recovering SAS-2 Zoning Assignments	342
Enabling Zoning and Creating SAS-2 Zoning Assignments	342
Chassis Hardware Requirements	343
▼ Access and Enable Sun Blade Zone Manager	343
▼ Allocating Storage to Entire Chassis: Quick Setup (Web)	345
▼ Allocate Storage Resources to Single Blade Server: Detailed Setup (Web)	347
▼ Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup (Web)	352
▼ Manually Create SAS-2 Zoning Allocations (CLI)	356
Managing Existing SAS-2 Storage Resource Allocations	358
▼ View Existing CPU Blade Server Storage Allocations (Web)	358
▼ Modify Existing Blade Group Allocations (Web)	361
▼ View and Modify Existing Storage Allocations (CLI)	365
Resetting Sun Blade Zone Manager Allocations to Factory Defaults	367
▼ Reset Zoning Allocations to Factory Defaults (Web)	367
▼ Reset Zoning Allocations to Factory Defaults (CLI)	368
Resetting the Zoning Password to Factory Default for Third-Party In-Band Management	368
▼ Reset the Zoning Password (Web)	368
▼ Reset the Zoning Password (CLI)	369
Index	371

Using This Documentation

- **Overview** – The Oracle ILOM Administrator's Guide for Configuration and Maintenance describes how to configure and manage Oracle hardware using the Oracle ILOM 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/E81115_01/index.html.

Feedback

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

Setting Up a Management Connection to Oracle ILOM and Logging In

Description	Links
Refer to this section for information about supported management connection options to Oracle ILOM.	■ “Establishing a Management Connection to Oracle ILOM” on page 17
Refer to this section for information about logging into Oracle ILOM, preconfigured user accounts, and supported operating systems and web browsers.	■ “Logging In to Oracle ILOM Server SP or CMM” on page 35
Refer to this section for a complete list of operating system web browsers that are supported by Oracle ILOM.	■ “Supported Web Browsers for Oracle ILOM” on page 40
Refer to this section for information on how to locate guidelines for enhancing Oracle ILOM security.	■ “Configuring Oracle ILOM for Increased Security” on page 40

Related Information

- Installation guide for Oracle servers or blade system CMM
- Administration guide for Oracle server
- *Oracle ILOM Security Guide*

Establishing a Management Connection to Oracle ILOM

The Oracle ILOM firmware arrives preconfigured on your Oracle server or chassis monitoring module (CMM) in a way that makes establishing a management connection to Oracle ILOM simple and straightforward.

For further details on how to establish a management connection to Oracle ILOM, see:

- [“Choosing and Configuring a Management Connection to Oracle ILOM” on page 18](#)
- [“Management Services and Network Default Properties” on page 33](#)

Choosing and Configuring a Management Connection to Oracle ILOM

Oracle ILOM supports the following management connections:

- [“Dedicated Network Management Connection \(Default\)” on page 18](#)
- [“Sideband Network Management Connection” on page 20](#)
- [“Dedicated Local Management Connection” on page 23](#)
- [“Dedicated Interconnect SP Management Connection” on page 24](#)

Dedicated Network Management Connection (Default)

All Oracle servers and CMMs that are shipped with Oracle ILOM provide a dedicated in-band management port on the chassis that securely segregates all management traffic away from the host.

All servers and CMMs arrive ready for you to establish a secure management connection to Oracle ILOM. Simply attach an active LAN connection to the physical network management port (NET MGT) on the chassis and you are ready to log in. For further instructions for setting up a dedicated management connection to Oracle ILOM, see the following procedure.

▼ Configure a Dedicated Network Management Connection to Oracle ILOM

Before You Begin:

- Review [“Management Services and Network Default Properties” on page 33](#).
- The Management Port property in Oracle ILOM is, by default, set to route all management traffic through the physical network management port (NET MGT) on the managed device.

Note - The dedicated network management connection is designed to be implemented independent of a sideband network management connection. However, either of these network management connections (dedicated or sideband) can coexist with the standard local serial management connection and (or) the internal high-speed interconnect management connection.

- To maintain the most reliable and secure environment for Oracle ILOM, the dedicated network management port on the server must always be connected to an internal trusted network or dedicated secure management/private network.

- The Management Port property for Oracle ILOM is configurable from the Oracle ILOM CLI and web interface. It is also configurable for x86 servers, from the BIOS Utility.
If you modify the Management Port property from Oracle ILOM, you must log in using either the default root account or a user account with Admin (a) role privileges. For log in instructions, see [“Log In to the Oracle ILOM SP or CMM” on page 36](#).

To verify or configure a dedicated network management connection to Oracle ILOM, follow these steps:

1. On the physical server or CMM verify that a LAN connection was established to the physical management port (NET MGT).

If a physical LAN connection to the NET MGT port is not established, attach an Ethernet cable between the network switch and the physical NET MGT port on the device. For further instructions, see the cabling section in the installation guide for the Oracle server or CMM.

Note - When an active LAN connection is attached to the NET MGT port on the managed server or CMM chassis, Oracle ILOM automatically detects an IP address for the SP or CMM from the IP routing device on your network. For guidelines for determining the IP address assigned to the Oracle ILOM SP or CMM, see [“Usage Guidelines for IP Network Management Address” on page 37](#).

2. Set the communication speed for the network switch port to auto-negotiate.

Note - If the network switch port speed is not set to auto-negotiate, you could experience a network communication error when connecting to Oracle ILOM.

3. To verify that the default Management Port property is set for the Oracle ILOM SP or CMM, perform the following steps using the applicable user interface.

User Interface	Step	Task: Verify or reset default management port property for SP or CMM
Oracle ILOM CLI	1:	Log in to the Oracle ILOM CLI and use the show command to view the network properties for the managed device, for example, type either: ■ <code>show /SP/network</code> ■ <code>show /CMM/network</code> For login instructions, see “Log In to the Oracle ILOM SP or CMM” on page 36 .
	2:	Verify that the /network output displays the default Management Port property for the SP or CMM, for example: ■ SP output: <code>managementport=MGMT</code> ■ CMM output: <code>switchconf=port0</code>

User Interface	Step	Task: Verify or reset default management port property for SP or CMM
	3:	If necessary, reset the default Management Port property for the SP or CMM. For SP, type: <pre>set /SP/network pendingmanagementport=MGMT commitpending=true</pre> For CMM, type: <pre>set /CMM/network pendingswitchconf=port0 commitpending=true</pre>
Oracle ILOM web interface	1:	Log in to the Oracle ILOM web interface and click ILOM Administration > Connectivity. For login instructions, see “Log In to the Oracle ILOM SP or CMM” on page 36.
	2:	In the Network Settings page, verify that the Management Port list box for the SP is set to MGMT or the CMM Management Network Switch list box is set to Port 0. If necessary, reset the default Management Port property by selecting MGMT for SP or Port0 for CMM, then click Save.
BIOS Setup Utility (only available for x86 servers)	1:	Access the BIOS Setup Utility on the managed x86 server, then in the BIOS Setup Utility dialog, click Advanced > IPMI 2.0 Configuration > Set LAN Configuration.
	2:	In the LAN Configuration menu, verify that the default Management Port property is set to MGMT. If necessary, reset the default Management Port property to MGMT, and then commit the change.

Related Information

- [“Modifying Default Connectivity Configuration Properties” on page 118](#)
- [“Setting Up and Maintaining User Accounts” on page 41](#)

Sideband Network Management Connection

For servers supporting sideband management, you can optionally connect to Oracle ILOM and manage the server remotely through the standard data port provided on the server chassis. Implementing a sideband management connection to Oracle ILOM eliminates the need to support two separate network connections for host and management traffic. However, this approach could: (1) potentially decrease the connection performance to Oracle ILOM, and (2) potentially provide risks for transmitting Oracle ILOM traffic over an untrusted network.

To configure Oracle ILOM to transmit management traffic through a sideband management connection, you must change the default Management Port property value (MGMT|port0) to the physical active data port (NET0, NET1, NET2, or NET3) on the server.

For further information about configuring a sideband management connection to Oracle ILOM, see the following:

- [“Configure a Sideband Management Connection to Oracle ILOM” on page 21](#)

- [“Sideband Management Network Connectivity Considerations” on page 22](#)

▼ Configure a Sideband Management Connection to Oracle ILOM

Before You Begin:

- Sideband management is supported on most Oracle servers. However, to verify whether a server supports sideband management, refer to the server administration guide or the product release notes.

Note - The sideband network management connection is designed to be implemented independent of a dedicated network management connection. However, either of these network management connections (dedicated or sideband) can coexist with the standard local serial management connection and (or) the internal high-speed interconnect management connection.

- Review [“Management Services and Network Default Properties” on page 33](#).
- To maintain the most reliable and secure environment for Oracle ILOM, the sideband management port on the server must always be connected to an internal trusted network or dedicated secure management or private network.
- The SP Management Port property for Oracle ILOM is configurable from the Oracle ILOM CLI and web interface. It is also configurable for x86 servers from the BIOS Setup Utility. If you modify the Management Port property through Oracle ILOM, the following requirements apply:
 - A management connection to Oracle ILOM should already be established. For instructions, see either:
 - [“Dedicated Network Management Connection \(Default\)” on page 18](#)
 - [“Dedicated Local Management Connection” on page 23](#)
 - You should have logged in to Oracle ILOM. For instructions, see [“Logging In to Oracle ILOM Server SP or CMM” on page 35](#).
 - The default root account or a user account with Admin (a) role privileges is required in Oracle ILOM to modify the Management Port property.

To configure a sideband management connection to Oracle ILOM, follow these steps:

1. **On the physical server, verify that an active LAN connection is established to the applicable Ethernet data port (NET0, NET1, NET2, or NET3).**

For instructions, refer to the cabling section in the server or blade system installation guide.

2. **To configure the SP Management Port property for sideband management, perform one of the following:**

- **From the Oracle ILOM web interface – Click ILOM Administration > Connectivity, then click the Management Port list box.**

In the Management Port list box, select the active physical data port name (NET0, NET1, NET2, or NET3), then click Save.

- **From the Oracle ILOM CLI – Type:**

```
set /SP/network pendingmanagementport=/SYS/MB/NETn commitpending=true
```

Where:

n is the physical active data port number (0, 1, 2, or 3) on the server.

- **From the BIOS Setup Utility (available for x86 servers) – Click Advanced > IPMI 2.0 Configuration > Set LAN Configuration.**

In the LAN Configuration menu, set the Management Port setting to the physical active data port name (NET0, NET1, NET2, or NET3), then click Commit for the change to take effect.

Note - For information about how to navigate, set, and save options in the host BIOS Setup Utility, see the administration guide provided for the server.

Related Information

- [“Sideband Management Network Connectivity Considerations” on page 22](#)
- [“Usage Guidelines for IP Network Management Address” on page 37](#)
- [“Modifying Default Connectivity Configuration Properties” on page 118](#)
- [“Recommended Practice for Spanning Tree Configurations ” on page 145](#)
- [“Setting Up and Maintaining User Accounts” on page 41](#)
- [“Assigning System Identification Information” on page 140](#)

Sideband Management Network Connectivity Considerations

This section provides general network connectivity issues for you to consider when using a sideband management connection to Oracle ILOM:

- In-chip connectivity between the server SP and the host operating system might not be supported by the on-board host Gigabit Ethernet controller. If this condition occurs, use

a different port or route to transmit the traffic between the source and destination targets instead of using L2 bridging/switching.

- Server host power cycles might cause a brief interruption of network connectivity for server Gigabit Ethernet ports (NET 0, 1, 2, 3) that are configured for sideband management. If this condition occurs, configure the adjacent switch/bridge ports as host ports.
- If the Ethernet data ports on the server are configured as switch ports and participate in the Spanning Tree Protocol (STP), you might experience longer outages due to spanning tree recalculations.

Dedicated Local Management Connection

All Oracle servers and CMMs arrive with a physical serial port on the chassis that makes it easy to establish a secure local management connection to Oracle ILOM. This type of management connection is particularly useful when a local console is the only way to access and diagnose system failures; or, when you need an alternative method for modifying the Oracle ILOM preconfigured network properties prior to establishing a LAN connection.

For further information about configuring a local serial management connection to Oracle ILOM, see the following procedure.

▼ Configure a Dedicated Local Management Connection to Oracle ILOM

Before You Begin:

- A local serial management connection to Oracle ILOM requires attaching a physical serial console device (text terminal, workstation, laptop, or a terminal emulator program) to the SER MGT port on the server or CMM.

For further information about the physical serial management port located on an Oracle Server, see the Oracle documentation provided for your server.

To configure a dedicated local management connection to Oracle ILOM, follow these steps:

1. **Attach a serial cable between the serial console device and the serial management (SER MGT) port on the server or CMM.**
2. **Set the console device communication properties to these values: 9600 baud, 8 bit, no parity, 1 stop bit.**

Note - If the transmit and receive signals are reversed (crossed over) for DTE to DTE communications, a null modem configuration is required. Use the adapter cable that is supplied with your system to achieve a null modem configuration.

3. **To create a connection between the console device and the Oracle ILOM SP or CMM, press Enter.**

Related Information

- [“Management Services and Network Default Properties” on page 33](#)
- [“Modifying Default Connectivity Configuration Properties” on page 118](#)
- [“Assignable Oracle ILOM User Roles” on page 43](#)
- [“Serial Management Port Owner” on page 98](#)
- [“Assigning System Identification Information” on page 140](#)

Dedicated Interconnect SP Management Connection

For Oracle servers supporting an internal Ethernet-over-USB interface, you can optionally establish a LAN management connection to Oracle ILOM from a host operating system (OS) client without the use of the network management (NET MGT) port on the server.

The LAN management connection is established through a link between the two ports on the installed Ethernet-over-USB interface: one connection point for the service processor and the other connection point for the host operating system (OS).

Some of the advantages you gain when implementing this type of management connection, are as follows:

- **Preconfigured non-routable IP addresses for easy deployment**

The local interconnect configuration arrives ready for automatic configuration using the preconfigured internal non-routable IP addresses for each internal connection point (ILOM SP and host OS).

Oracle ILOM presents the Ethernet-over-USB interface that is installed on a managed server as a traditional “Ethernet” interface.

- **A secure authenticated local connection to Oracle ILOM**

Connecting to Oracle ILOM over the local interconnect requires user authentication just as if the connection were being established to Oracle ILOM through a dedicated or sideband network management connection.

All operating system users with a valid user name and password are permitted access to Oracle ILOM.

- **A fast alternative for local management**

Perform all Oracle ILOM management tasks over an internal high-speed dedicated management connection.

A local interconnect management connection provides a faster alternative for locally managing the server than using a traditional local serial console or a host Keyboard Controller Style (KCS) interface.

For further information about establishing a local interconnect connection to the Oracle ILOM SP, see these topics:

- [“Configuration Methods for Local Interconnect” on page 25](#)
- [“Manually Configure the Local Interconnect” on page 27](#)
- [“Host OS Interconnect Guidelines for Manual Configuration” on page 30](#)
- [“Oracle ILOM SP Interconnect Properties” on page 31](#)

Configuration Methods for Local Interconnect

To establish a dedicated LAN management connection between the host OS and the Oracle ILOM SP, you must choose to implement one of the following configuration methods:

- **Auto-Configuration (default)** — The configuration of the local interconnect management connection is automated when: 1) the Host Managed check box in the Oracle ILOM web interface is enabled (or hostmanaged property in the CLI is set to true (`/SP/network/interconnect hostmanaged=true`)); and, 2) the Ethernet-over-USB interface is enabled by one of the following software products:
 - Oracle Solaris version 11.x or later. Typically, the option for Ethernet-over-USB is enabled at first OS boot.
 - or-
 - MS Windows or a Linux-based operating system that supports the use of an internal Ethernet-over-USB device.
 - or-
 - Oracle Hardware Management Pack version 2.1.0 or later.
- **Manual-configuration** — If you are an advanced network administrator and prefer not to have Oracle ILOM auto-configure the Ethernet-over-USB connection points, you can manually configure the local host connection point addresses by using the `ilomconfig` tool .

Note - The `ilomconfig` tool is part of Oracle Solaris, no installation is required. For MS Windows or Linux-based operating system environments, the `ilomconfig` tool is available for installation from the Oracle Hardware Management Pack version 2.1.0 or later. Alternatively, advanced network administrators can use OS networking commands to configure the Ethernet-over-USB connection points.

For manual configuration details, see [“Manually Configure the Local Interconnect” on page 27](#).

▼ Auto-Configure a Dedicated Interconnect Management Connection

Before You Begin:

- The Ethernet-over-USB interface must be enabled by the installed operating system.
- The Admin (a) role is required to configure the Local Host Interconnect feature.

Follow these steps to auto-configure a dedicated interconnect management connection using the Oracle ILOM CLI or web interface.

Note - Alternatively, you can set the auto-configure Ethernet-over USB connection point addresses by using the `ilomconfig` tool. For more details, see the [“Manually Configure the Local Interconnect” on page 27](#).

1. **Ensure that the Ethernet-over-USB interface is enabled by the installed operating system or by the installation of the Oracle Hardware Management Pack software version 2.1.0 or later.**
2. **To navigate to the Local Host Interconnect properties, perform one of the following:**
 - **Web:** Click Connectivity > Network then click the Local Host Interconnect link at top of page.
 - If a Configure link appears, click the Configure link.
 - If a Host Interconnect Node table appears, select a Host then click Edit.The Local Host Interconnect Parameters dialog appears.
 - **CLI:** Type: `cd /SP/network/interconnect`
3. **Ensure that the Host Managed property is set to True.**

Note - Disabling the Host Managed property (`hostmanaged=false`) after an internal management connection is auto-configured by Oracle ILOM will cause all host applications running on the auto-configured internal management connection to fail.

For further configuration details, see [“Oracle ILOM SP Interconnect Properties” on page 31](#).

▼ Manually Configure the Local Interconnect

Note - Alternatively, you can use the Oracle Hardware Management Pack 2.1.0 software or later to auto-configure the Local Interconnect connection points on a managed server. For local interconnect auto-configuration instructions, see the *Oracle Hardware Management Pack User's Guide*.

Before You Begin:

- This manual procedure for configuring a local interconnect between the SP and host OS should be performed only by advanced users.
- This manual procedure provides guidelines for configuring the host OS internal connection point and detailed steps for optionally configuring the Oracle ILOM SP internal connection point.
- An established network or local serial management connection is required to the Oracle ILOM SP prior to modifying the default SP Local Host Interconnect properties in Oracle ILOM.

Note - The Local Host Interconnect property in Oracle ILOM is not available for a CMM. However, you can use the Oracle ILOM CMM CLI or web interface to navigate to and configure the SP Local Host Interconnect properties for any blade server installed in the chassis.

- The preconfigured Oracle ILOM root account or a customer-configured user account with Admin (a) role privileges is required to modify the SP Local Host Interconnect properties in Oracle ILOM.
- Prior to performing this procedure, verify that an interconnect management connection between the SP and host OS was not automatically configured by Oracle ILOM. In the case an interconnect management connection was auto-configured by Oracle ILOM, disabling the host managed property (`hostmanaged=false`) using the procedure below will cause the local host applications running on the auto-configured interconnect management connection to fail.

Follow these steps to manually configure the internal Ethernet USB connection points between the host OS and the Oracle ILOM SP:

1. **To manually configure the internal Ethernet USB connection parameters for the host operating system, do the following:**
 - a. **Ensure that the OS specific Ethernet device driver was installed by the OS software distribution on the managed server.**

If an OS specific Ethernet device driver was not provided during the operating system installation, you can obtain the device driver for the internal Ethernet-over-USB interface from the Oracle Hardware Management Pack 2.1.0 or later software distribution. For more information about how to extract this file from the Oracle Hardware Management Pack software distribution, refer to the *Oracle Hardware Management Pack User's Guide*.

- b. **Confirm that the host operating system on the managed server recognizes the internal Ethernet-over-USB interface, and then manually assign network parameters to the host OS connection point.**

For guidelines, see [“Host OS Interconnect Guidelines for Manual Configuration” on page 30](#).

2. **To manually modify the Local Host Interconnect properties for the Oracle ILOM SP, follow these steps:**

- a. **Review [“Oracle ILOM SP Interconnect Properties” on page 31](#).**

- b. **Log in to Oracle ILOM using a web browser or a CLI shell.**

For log in instructions see, [“Logging In to Oracle ILOM Server SP or CMM” on page 35](#).

- c. **To modify the SP Local Host Interconnect properties in Oracle ILOM, perform the following steps for the applicable Oracle ILOM interface.**

Oracle ILOM Interface	Steps:
Web	1. In the Oracle ILOM SP web interface, click ILOM Administration > Connectivity > Network, and then click the Local Host Interconnect link at the top of the page. 2. In the Local Host Interconnect section of the Network page, do one of the following: ■ Click the Configure link -or- ■ Select a host from the table and click Edit. 3. In the Local Host Interconnect Parameters dialog, clear the check box for Host Managed, enable the check box for State, specify the allowed communication services, and only if necessary, modify the local non-routable IPv4 address or netmask addresses provided for the SP, then click Save. For further configuration details, see the “Oracle ILOM SP Interconnect Properties” on page 31. Note. You do not need to modify the preconfigured IP address or netmask address assigned to the Oracle ILOM SP, unless a conflict with these parameters exists in your network.
CLI	1. Navigate to the <code>/network/interconnect</code> working directory on the managed server. For example: From a single server SP CLI, type: <code>cd /SP/network/interconnect</code>

Oracle ILOM Interface	Steps:
	From a CMM CLI, type: cd /Servers/Blades/BLn/network/interconnect From a multi-domain server SP CLI, type: cd /Servers/PDomains/PDomain_n/SP/network/interconnect 2. To disable the <code>hostmanaged</code> property and to enable the Local Host Interconnect state, type : set hostmanaged=false set state=enabled Note. You do not need to modify the preconfigured non-routable IP address and netmask address assigned to the Oracle ILOM SP, unless a conflict with these parameters exists in your network. 3. Set the allowed_services communication property. For further configuration details, see “Oracle ILOM SP Interconnect Properties” on page 31 4. To modify the local non-routable IPv4 address or netmask address provided for the SP, type: set pendingipaddress=specify_new_address set pendingipnetmask=specify_new_address set commitpending=true

3. To test the local interconnect management connection between the host OS and the Oracle ILOM SP, perform any of the following:

- On the managed server host operating system, using a web browser or a CLI shell, log in to the Oracle ILOM SP by entering the non-routable IP address that is assigned to the SP USB Ethernet connection point.

Expected results for:

Web browser connection – The Oracle ILOM Login page appears.

CLI shell connection – An authorization prompt for Oracle ILOM appears.

- Ping the local interconnect SP address from the host OS.

For instructions, see [“Test IPv4 and IPv6 Connectivity” on page 145](#).

Related Information

- [“Host OS Interconnect Guidelines for Manual Configuration” on page 30](#)
- [“Oracle ILOM SP Interconnect Properties” on page 31](#)
- [“Logging In to Oracle ILOM Server SP or CMM” on page 35](#)
- [“Oracle ILOM Deployment Practices for Increasing Security” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x](#)
- Oracle Hardware Management Pack Document Library at: <http://www.oracle.com/pls/topic/lookup?ctx=ohmp>

Host OS Interconnect Guidelines for Manual Configuration

The following table provides general guidelines for configuring local network parameters for the host OS internal USB Ethernet connection point.

Note - The internal USB Ethernet installed on the managed server is presented in the system as a traditional ethernet interface. When manually configuring the local interconnect point for the host OS, it might be necessary to use the host MAC address (`hostmacaddress=`) to determine the name assigned to the host OS local interconnect point.

TABLE 1 Host OS Interconnect Manual Configuration Guidelines

Operating System	Manual Host OS Interconnect Guidelines
MS Windows or Linux-based operating system	1. Ensure that the internal Ethernet-over-USB device is automatically discovered by operating system. 2. Install the <code>ilomconfig</code> tool. This tool is included in the Oracle Hardware Management Pack software distribution. Note - As an alternative to using the <code>ilomconfig</code> tool, you can use OS networking commands to configure the internal Ethernet-over-USB connection point addresses. 3. In the <code>ilomconfig</code> tool, do one of the following: ■ Manually set the connection point addresses for the internal Ethernet-over-USB interface: <pre>ilomconfig enable interconnect --spipaddress=x.x.x.x --netmask=x.x.x.x --hostipaddress=x.x.x.x</pre> -or- ■ Manually set the default connection point addresses for the internal Ethernet-over-USB interface: <pre>ilomconfig enable interconnect</pre>
Solaris	1. Ensure that the internal Ethernet-over-USB device is automatically discovered by Oracle Solaris. 2. In the <code>ilomconfig</code> tool, do one of the following: Note - The <code>ilomconfig</code> tool is part of Oracle Solaris, no installation is required. ■ Manually set the connection point addresses for the internal Ethernet-over-USB interface: <pre>ilomconfig enable interconnect --spipaddress=x.x.x.x --netmask=x.x.x.x --hostipaddress=x.x.x.x</pre> -or- ■ Manually set the default connection point addresses for the internal Ethernet-over-USB interface: <pre>ilomconfig enable interconnect</pre>

Oracle ILOM SP Interconnect Properties

The following table describes the SP Local Host Interconnect properties appearing in the Oracle ILOM CLI (target: /network/interconnect) and the Oracle ILOM web interface (ILOM Administration > Connectivity > Local Host Interconnect > Configure).

TABLE 2 Oracle ILOM SP Interconnect Properties

Property	Default Value	Description
Host Managed (hostmanaged=)	Enabled (True)	<i>Enabled (True) Disabled (False)</i> Specify the option for configuring the USB Ethernet connection points: ■ Enabled True (default) - To enable, select the Host Managed check box to instruct Oracle ILOM to auto-configure the link between the SP port and host-side port on the installed Ethernet-over-USB interface. Note - Disabling the Host Managed property (hostmanaged=false) after an internal management connection is auto-configured by Oracle ILOM will automatically cause all the host applications running on the auto-configured internal management connection to fail. ■ Disabled False - To disable, clear the Host Managed check box to instruct Oracle ILOM not to configure the link between the SP port and host port on the installed Ethernet-over-USB interface. When the Host Managed check box is set to False, advanced network administrators can optionally configure the Ethernet-over-USB connection manually. Single SP CLI Syntax <pre>set /SP/network/interconnect hostmanaged=true false</pre> CMM-Blade CLI Syntax <pre>set /Servers/Blades/BL/network/interconnect hostmanaged=true false</pre> Multi-Domain SP CLI Syntax <pre>set /Servers/PDomains/PDomain_n/SP/network/interconnect hostmanaged=true false</pre>
State (state=)	Disabled	<i>Enabled Disabled (default)</i> When the Host Managed property is set to False (check box is cleared), specify one of the following State modes: ■ Disabled (default) - Clear the State check box to disable the Local Host Interconnect (USB Ethernet link interface) feature in Oracle ILOM ■ Enabled - Select the State check box to enable the Local Host Interconnect (USB Ethernet link interface) feature in Oracle ILOM.

Property	Default Value	Description
		Note - If you choose to manually configure the Ethernet-over-USB connection points between the host OS and the Oracle ILOM SP, the value for this property must be set to enabled. Single SP CLI Syntax set /SP/network/interconnect state=enabled disabled CMM-Blade CLI Syntax set /Servers/Blades/BL/network/interconnect state=enabled disabled Multi-Domain SP CLI Syntax set /Servers/PDomains/PDomain_n/SP/network/interconnect state=enabled disabled
IP Address (pendingipaddress=)	169.254.182.7	When the Host Managed is set to False, you can optionally modify the non-routable IPv4 address for the service processor USB Ethernet connection. Note - By default, Oracle provides non-routable IPv4 addresses for each connection point (ILOM service processor and host OS). Do not change these addresses unless a conflict exists in your network environment with the provided non-routable IPv4 addresses.
Netmask Address (pendingipnetmask=)	255.255.255.0	When the Host Managed check box is set to False, you can optionally modify the network mask Note - You typically will not need to change the preconfigured IPv4 Netmask (255.255.255.0) address, unless a conflict with this address exists in your network. CLI Syntax set pendingipaddress=specify_new_address set pendingipnetmask=specify_new_address
Allowed Services (allowed_services=)	Fault-Transport, IPMI, SNMP	Fault-Transport, IPMI, SNMP (defaults) HTTP, HTTPS, SSH Note - The Allowed Services property is available for configuration as of Oracle ILOM firmware version 3.2.6. When the Host Managed is set to False, you can optionally modify the list of allowed communication services. Any combination of services is allowed. Web - Allowed Services To enable a single communication service, click the name of a communication service in the list. To enable multiple communication services, press the Ctrl key as you click the names of the communication services in the list. To disable one or more communication services, press the Ctrl key as you click the names of the highlighted (enabled) communication services in the list. CLI Syntax - Allowed Services

Property	Default Value	Description
		Single SP CLI example: set /SP/network/interconnect allowed_services=fault-transport, http, https, ipmi, snmp, ssh
Save (commitpending=true false)		Any modifications made to IP Address or Netmask Address for the Oracle ILOM SP Ethernet-over-USB connection point are considered pending until the changes are committed in the CLI or saved in the web interface. CLI Syntax set commitpending=true
Service Processor MAC Address (spmaddress=)	Read-only	The read-only property for the Service Processor MAC Address displays the MAC address that is assigned to the Oracle ILOM SP.
Host MAC Address (hostmacaddress=)	Read-only	The read-only property for the Host MAC Address displays the MAC address that is assigned to the managed server and it also represents how most operating systems recognize the internal Ethernet-over-USB interface.
Connection Type	Read-only	This read-only Connection Type property indicates the connection type of the internal USB Ethernet.
CLI help command		For additional information about configurable or non-configurable properties appearing under the /network/interconnect CLI target, you can type the help command followed by the property name. Syntax: help /SP CMM/network/interconnect <i>property_name</i> Example: help /SP/network/interconnect hostmanaged
More details ... (web help)		For additional information, click the More details link in the Local Host Interconnection section of the Connectivity > Network page.

Management Services and Network Default Properties

To help make the process for deploying a server simple and straightforward, Oracle ILOM is shipped preconfigured with most management service ports and standard network connectivity properties enabled. However, to maximize security and to prevent unauthorized access to Oracle ILOM, you should disable properties for any management service ports that are not required.

Note - The default properties in Oracle ILOM are customer-configurable after establishing a management connection to Oracle ILOM.

- [Table 3, “Management Services Enabled by Default ,” on page 34](#) Management Services Enabled by Default

- [Table 4, “Network Connectivity Properties Enabled by Default,” on page 35](#) Network Connectivity Properties Enabled by Default

TABLE 3 Management Services Enabled by Default

Management Access	Default Properties	Service Port	To modify configurable properties, see;
Web Server: Mode	■ Redirect HTTP Connection to HTTPS	80	Table 38, “Web Server Configuration Properties,” on page 101
Web Server: State	■ HTTPS, Enabled	443	Table 38, “Web Server Configuration Properties,” on page 101
Web Server: SSL	Later firmware versions of Oracle ILOM) ■ TLS v1.1 Disabled Note - Support for TLSv1.0 is removed as of Oracle ILOM 4.0.0 Note - TLSv1.1 is disabled by default as of Oracle ILOM 4.0.4. ■ TLS v1.2 Enabled ■ Default SSL certificate ■ Default SSL self-signing private key	-	Table 39, “SSL Certificate and Private Key Configuration Properties for HTTPS Web Server,” on page 104
IPMI: State	■ Enabled	623	Table 42, “IPMI Service Configuration Properties,” on page 112 Note. For a higher level of security, Oracle ILOM IPMI clients should always support and operate in IPMI 2.0 mode.
SNMP: State	■ SNMPv3, Enabled	161	Table 40, “SNMP Configuration Properties,” on page 107
Single Sign On	■ Enabled	11626	“Single Sign-On Service (Enabled by Default)” on page 45
Secure Shell (SSH)	■ Enabled ■ RSA and DSA Key Generation	22	Table 41, “SSH Server Configuration Properties,” on page 110
Remote KVMS Redirection (video, keyboard, mouse, and storage)	■ Enabled	5120-5123, 5555, 5556, 7578, 7579	“Using Remote KVMS Consoles for Host Server Redirection” on page 147
Service tag [†]	■ Enabled	6481	Table 45, “Servicetag Service Configuration Properties,” on page 118

[†]An Oracle discovery protocol that identifies servers and provides integration to Oracle service solutions.

Note - For a complete list of default network ports used by Oracle ILOM, see [“Default Network Ports Used by Oracle ILOM” on page 99](#).

TABLE 4 Network Connectivity Properties Enabled by Default

Network Connectivity Property	Default Value	To modify configurable properties, see:
Network: State	■ Enabled	Table 46, “Network Connectivity Standard Configuration Properties,” on page 119
IPv4: Mode	■ DHCP, enabled	
IPv6: State	■ Enabled	Table 46, “Network Connectivity Standard Configuration Properties,” on page 119
IPv6: Mode	■ Auto-Config, Stateless	
Management Port:	■ Dedicated Network Management (MGMT)	Table 46, “Network Connectivity Standard Configuration Properties,” on page 119
Local Host Interconnect	■ Host Utilities Managed: Enabled ■ State: Disabled	“Dedicated Interconnect SP Management Connection” on page 24
DNS	■ Auto DNS via DHCP, Enabled	Table 48, “DNS Configuration Properties,” on page 134
Serial Port	■ Owner: Service Processor ■ Baud Rate: 9600 ■ Host Flow Control: None	Table 49, “Serial Port Configuration Properties,” on page 136
User Authentication [†]	■ Root user account: root ■ Root password: changeme ■ Permitted local accounts: Up to 10 customer-configurable user accounts ■ Single Sign On: Enabled for remote KVMs and CMM blade navigation (drill-down).	“Managing User Credentials” on page 41

[†]The property states for LDAP, RADIUS, and Active Directory are, by default, disabled.

Logging In to Oracle ILOM Server SP or CMM

Oracle ILOM comes with a preconfigured user account and default network parameters that simplifies logging in to Oracle ILOM for the first time. For further information about logging in to Oracle ILOM, see these topics:

- [“Log In to the Oracle ILOM SP or CMM” on page 36](#)
- [“Usage Guidelines for IP Network Management Address” on page 37](#)
- [“Preconfigured User Accounts Enabled by Default” on page 38](#)
- [“Supported Web Browsers for Oracle ILOM” on page 40](#)

▼ Log In to the Oracle ILOM SP or CMM

Before You Begin

- An established local or network management connection to Oracle ILOM is required.
For instructions, see [“Choosing and Configuring a Management Connection to Oracle ILOM” on page 18](#).
- The preconfigured Oracle ILOM `root` account or a customer-configured user account is required to log in to Oracle ILOM.
For information about the preconfigured `root` account, see [“Preconfigured User Accounts Enabled by Default” on page 38](#). For information about how to create user accounts in Oracle ILOM, see [“Managing User Credentials ” on page 41](#).

To log in to Oracle ILOM from a local serial management connection or a network management connection, follow these steps:

1. **To log in to Oracle ILOM, perform the following steps for the applicable Oracle ILOM interface:**

Oracle ILOM Interface	Steps
Local serial console (SER MGT port)	■ After creating a connection between the console and Oracle ILOM by pressing Enter, type the Oracle ILOM user name and password when prompted. For example: Type <code>root</code> for user name and <code>changeme</code> for password.
Web browser	1. Type <code>http://ILOM_SP_or_CMM_ipaddress</code> into the web browser and press Enter. The Oracle ILOM Login page appears. For guidelines for entering the IP address assigned to Oracle ILOM, see “Usage Guidelines for IP Network Management Address” on page 37. 2. Log in to the Oracle ILOM web interface by specifying a valid Oracle ILOM user name and password. For example: Type <code>root</code> for user name and <code>changeme</code> for password. The Oracle ILOM Summary page appears.
CLI secure shell	1. To establish an SSH session to the Oracle ILOM CLI, open a terminal window. 2. To log in to Oracle ILOM using the default <code>root</code> account, type: <code>\$ ssh root@ILOM_SP_or_CMM_ipaddress</code> Oracle ILOM prompts you for the <code>root</code> password. 3. At the Password prompt, type <code>changeme</code>. The Oracle ILOM CLI prompt appears (<code>-></code>). To access a blade server SP from the CMM CLI, refer to the “Managing Blade Servers From the CMM CLI” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x.

2. To exit Oracle ILOM, perform one of the following:

- To exit the Oracle ILOM web interface session – Click the Log Out button located in the upper right side of the web interface page.
- To exit the Oracle ILOM CLI session – Type: `exit`

Related Information

- [“Assigning System Identification Information” on page 140](#)
- [“Default Timeout for CLI and Web Sessions” on page 93](#)
- [“Modifying Default Management Access Configuration Properties” on page 100](#)
- [“Management of Banner Messages at Log-In” on page 94](#)
- [“Setting Up and Maintaining User Accounts” on page 41](#)
- [“Password Recovery for Default root Account” on page 49](#)
- [“Setting Up a Management Connection to Oracle ILOM and Logging In” on page 17](#)
- [“Using Remote KVMs Consoles for Host Server Redirection” on page 147](#)
- [“Viewing System Inventory, Health, and Performing Service and Management Actions” in *Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*](#)
- [“CLI Reference for Mapping Management Tasks to CLI Targets” in *Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*](#)
- [“Updating Oracle ILOM Firmware” on page 293](#)

Usage Guidelines for IP Network Management Address

The following table provides guidelines to help determine: (1) the IP address assigned to the Oracle ILOM SP or CMM based on default network properties, (2) the accepted IPv6 syntax, and 3) a list of non-supporting IPv6 servers.

TABLE 5 IP Address Identification, IPv6 Accepted Syntax, Non-supporting IPv6 servers

To determine:	Guidelines
IP address assigned to Oracle ILOM	To determine the assigned IP address, perform these steps. 1. Establish a local serial management (SER MGT) connection to the ILOM SP or CMM. 2. Log in to Oracle ILOM 3. Use the show command to view the IP network properties under: /SP/network for the current IPv4 address assigned to Oracle ILOM. /SP/network/ipv6 for the current IPv6 address assigned to Oracle ILOM.

To determine:	Guidelines
	You can also determine the IP address from the IPv4 DHCP server or the IPv6 routing device on your network.
Accepted syntax for IPv6 network address	- When entering the URL in a web browser, the IPv6 address <i>must be enclosed</i> in brackets to work correctly. For example: https://[ipv6address] - When establishing an Oracle ILOM CLI session using SSH, the IPv6 address <i>should not be enclosed</i> in brackets. For example: ssh root@ipv6address - When transferring a file using the CLI load -source command and tftp, the IPv6 address <i>must be enclosed</i> in brackets. For example: load -source tftp://[ipv6address]filename.extension
Legacy Oracle servers not supporting IPv6	Oracle's SPARC servers: - T5440 - T5220 - T5120 - T5140 - T5240 - T6340 Oracle's Sun Fire servers: - X4140 - X4150 - X4240 - X4440 - X4450 - X4600 - X4600 M2 - X4640

Preconfigured User Accounts Enabled by Default

Oracle ILOM arrives with a preconfigured Administrator user account known as `root`, and a password-recovery user account known as `default`. For further information about the use of these accounts, see the following table.

TABLE 6 Local User Accounts Enabled by Default

Preconfigured User Account	Default Login Properties	Description	To modify, see:
root	Username: root	The Oracle ILOM root user account is a persistent local user account that is available on all Oracle ILOM interfaces [†] , unless, you choose to delete the persistent root user account.	“Managing User Credentials” on page 41

Preconfigured User Account	Default Login Properties	Description	To modify, see:
	■ Password: changeme	Built-in administrative privileges – The root account includes built-in administrative privileges (read and write) for all Oracle ILOM features, functions, and commands. Recommended security practice – To prevent unauthorized access to the managed server or CMM, you should either: ■ Modify the default root password (changeme) provided on each Oracle ILOM service processor (SP) or chassis monitoring module (CMM). - or - ■ Delete the preconfigured root account provided on the Oracle ILOM SP and Oracle ILOM CMM. Prior to removing the preconfigured root account, you must replace the root account with a customer-configurable local user account or a directory service such as LDAP or Active Directory. Note. When the root account password is set to changeme (default password), a warning message appears in the CLI upon logging in and a warning message appears in the top portion of the web interface page.	
default	■ Username: default ■ Password: defaultpassword	The preconfigured default user account provided in Oracle ILOM is limited to password recovery. Local serial console use only – The preconfigured default user account is available for use through a local serial connection only. Also, you must be able to prove physical presence at the server or CMM. Usage Scenario – If you delete the root account in Oracle ILOM prior to replacing the root account with a customer-configurable account, you can use the default account to log in to Oracle and use the normal Oracle ILOM commands to create a new account. Related Information: ■ Table 13, “Recover Preconfigured root Account or root Account Password (CLI only),” on page 49 ■ (Physical Presence) “Assigning System Identification Information” on page 140	“Password Recovery for Default root Account” on page 49

[†]Oracle ILOM web interface, CLI shell, local serial console, and IPMI.

Supported Web Browsers for Oracle ILOM

Oracle ILOM supports the use of the following web browsers on the SP, CMM, Oracle ILOM Remote System Console, and the Oracle ILOM Remote System Console Plus. Note that other web browsers that were not tested and are not listed in the following table might also be compatible with Oracle ILOM for monitoring and managing remote devices.

TABLE 7 Supported Web Browsers for Oracle ILOM

Operating System	Web Browser
Oracle Solaris 10 and 11	■ Mozilla Firefox ESR 45.2
Oracle Linux 7, Red Hat Enterprise Linux 7, SuSE Linux Enterprise 12, Ubuntu Linux LTS 14	■ Mozilla Firefox 38.1 and 45.3
Microsoft Windows 7	■ Google Chrome 55.0.2987, 58.0.3029.81 ■ Internet Explorer 11.0.41, 11.0.9600 ■ Mozilla Firefox ESR 52.2.0
Microsoft Windows 10	■ Google Chrome 59.0.3071.115 ■ Internet Explorer 11.0.43 ■ Mozilla Firefox ESR 52.2.0
Apple Mac OS X 10.7 through 10.11 ^{†‡}	■ Safari 10.0

[†]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.

[‡]The Oracle ILOM Remote System Console Plus is not supported on Macintosh browser clients.

Configuring Oracle ILOM for Increased Security

All configurable properties in Oracle ILOM can be optionally disabled or enabled to make the Oracle ILOM management environment more secure. For further details about enhancing security in Oracle ILOM, refer to the security guidelines described in the [Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x](#).

Setting Up and Maintaining User Accounts

Description	Links
Refer to this section for authentication configuration options, user role privileges, single sign-on service, permitted user sessions, SSH key configuration, or changing or recovering the preconfigured root account and password.	■ “Managing User Credentials” on page 41
Refer to this section for requirements and instructions for configuring local user accounts in Oracle ILOM.	■ “Configuring Local User Accounts” on page 51
Refer to this section for information about configuring the Password Policy for all local user accounts.	■ “Managing Password Policy Restrictions for Local Users” on page 53
Refer to this section for requirements and instructions for configuring Oracle ILOM as an Active Directory client.	■ “Configuring Active Directory” on page 59
Refer to these sections for requirements and instructions for configuring Oracle ILOM as an LDAP/SSL client or LDAP client.	■ “Configuring LDAP/SSL” on page 69 ■ “Configuring LDAP” on page 79
Refer to this section for requirements and instructions for configuring Oracle ILOM as a RADIUS client.	■ “Configuring RADIUS” on page 82

Related Information

- [“Oracle ILOM Deployment Practices for Increasing Security” in *Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x*](#)
- [“Preconfigured User Accounts Enabled by Default” on page 38](#)

Managing User Credentials

User access to Oracle ILOM is controlled by authenticated user accounts. Authorization to use discrete features within Oracle ILOM are managed through a set of user roles assigned to an Oracle ILOM user account.

When setting up user credentials in Oracle ILOM for the first time, system administrators can choose to configure up to 10 local user accounts, or choose to configure a centralized authentication service to permit additional user accounts.

For further details about supported user credential configuration options in Oracle ILOM, as well as general details about managing user credentials in Oracle ILOM, see the following topics:

- [“Supported User Authentication Configuration Options” on page 42](#)
- [“Assignable Oracle ILOM User Roles” on page 43](#)
- [“Single Sign-On Service \(Enabled by Default\)” on page 45](#)
- [“Maximum Number of User Sessions Supported” on page 46](#)
- [“Manage User Authenticated Sessions per Managed Device” on page 46](#)
- [“CLI Authentication Using Local User SSH Key ” on page 48](#)
- [“Security Action: Change Default root Account Password” on page 49](#)
- [“Password Recovery for Default root Account” on page 49](#)
- [“Supported File Transfer Methods” on page 50](#)

Supported User Authentication Configuration Options

Before choosing and configuring how you want to implement user authentication in Oracle ILOM, consider the following information.

TABLE 8 User Authentication Configuration Options

Option	Features and Considerations
Local User Account Authentication	■ Up to 10 configurable user accounts stored locally in Oracle ILOM. ■ Two preconfigured user accounts are shipped for quick deployment and maintenance: root user account and default user account (see “Preconfigured User Accounts Enabled by Default” on page 38). ■ Configurable user role privileges granting either read-only or read and write access to discrete Oracle ILOM features (see “Assignable Oracle ILOM User Roles” on page 43). ■ Secure user authentication and authorization for local and remote management. ■ Oracle ILOM user credentials are maintained separately for each SP and CMM. For additional information about configuring local user accounts in Oracle ILOM, see “Configuring Local User Accounts ” on page 51.
Authentication Directory Service	■ Provides users access to Oracle ILOM beyond 10 local user accounts. ■ Enables system administrators to centrally create and maintain user credentials for all Oracle ILOM instances (all managed server SPs and CMMs in local network environment). ■ Enables authenticated Oracle ILOM users to have access to all Oracle ILOM instances.

Option	Features and Considerations
	■ Enables system administrators to configure user authentication rules for using features within Oracle ILOM.

TABLE 9 Supported Authentication Directory Services

Authentication Service	Description
Active Directory	Active Directory is a distributed service that is provided with Microsoft Windows Server operating systems. The Active Directory service is secure by default. For additional information about configuring Oracle ILOM to use the Active Directory authentication service, see “Configuring Active Directory ” on page 59.
LDAP/SSL	The LDAP/SSL authentication service is secure by default. It supports an optional strict certification mode that requires the use of a security certificate. For information about configuring Oracle ILOM as an LDAP/SSL client, see “Configuring LDAP/SSL” on page 69.
LDAP	The LDAP (v2) authentication service is less secure than LDAP/SSL. Configure this service only if you understand and accept the security limitations. For additional information about configuring Oracle ILOM as a LDAP client, see “Configuring LDAP” on page 79.
RADIUS	Remote Authentication Dial In User Service (RADIUS) is a networking protocol that uses a client-server model to provide user authentication and authorization. For additional information about configuring Oracle ILOM to use the RADIUS authentication service, see “Configuring RADIUS ” on page 82.

Assignable Oracle ILOM User Roles

During the creation of Oracle ILOM user accounts, a system administrator assigns a set of privileges that grants users access to discrete functions and operations within Oracle ILOM. These privileges in Oracle ILOM are known as *user roles*.

Oracle ILOM provides up to six predefined user roles. A system administrator can assign roles to grant privileges to a user or to revoke privileges from a user.

In addition to user roles, Oracle ILOM provides user profiles known as Administrator, Operator, and Advanced Roles. These user profiles enable a system administrator to assign multiple privileges at a time to a single user.

A system administrator can use the Administrator or Operator profile to assign a set of predefined user roles to a single user account. Or, a system administrator can configure the Advanced Roles profile to assign any of the six predefined user roles to a single account.

All user privileges are assignable to a user account from the web interface or the CLI. For a description of privileges granted by a single profile or a user role, see the following tables:

- [Table 10, “Privileges Granted by a User Profile,” on page 44](#) Privileges Granted by a User Profile
- [Table 11, “Privileges Granted by Individual User Roles,” on page 45](#) Privileges Granted by Individual User Roles

TABLE 10 Privileges Granted by a User Profile

Web Property	CLI Property	Privileges Granted by Profile
Administrator	administrator	The Administrator (administrator) profile is predefined with the following user roles. ■ Admin (a) ■ User Management (u) ■ Console (c) ■ Reset and Host Control (r) ■ Read-Only (o) For a description of privileges granted by each user role, see Table 11, “Privileges Granted by Individual User Roles,” on page 45.
Operator	operator	The Operator (operator) profile is predefined with the following user roles: ■ Console (c) ■ Reset and Host Control (r) ■ Read-Only (o) For a description of privileges granted by each user role, see Table 11, “Privileges Granted by Individual User Roles,” on page 45.
Advanced Roles	a u c r o s	The Advanced Roles profile option is user-configurable from the web interface only. The Advanced Roles profile option enables system administrators to assign any of the following six user roles to a single user account: ■ Admin (a) ■ User Management (u) ■ Console (c) ■ Reset and Host Control (r) ■ Read-Only (o) ■ Service (s) Note - The same six user roles (a u c r o s) are individually assignable to a single user account from the CLI. For a description of privileges granted by each user role, see Table 11, “Privileges Granted by Individual User Roles,” on page 45.

TABLE 11 Privileges Granted by Individual User Roles

User Role	Privileges Granted
Admin (a)	The Admin (a) user role, when enabled, grants read and write permissions to all Oracle ILOM system management functions with the exception of the functions that would require the Admin (a) role to have these additional user roles enabled: User Management (u), Reset and Host Control (r), Console (c), and Service (s).
User Management (u)	The User Management (u) user role, when enabled, grants read and write permissions to all Oracle ILOM user management authentication features.
Console (c)	The Console (c) user role, when enabled, grants read and write permissions to perform these remote console management functions: remote console lock options, SP console history log options, launch and use Oracle ILOM Remote System Console, and launch and use Oracle ILOM Storage Redirection CLI.
Reset and Host Control (r)	The Reset and Host Control (r) user role, when enabled, grants read and write permissions to perform these host management functions: host boot device control, run and configure diagnostics utilities, reset SP, reset CMM, sub-component service actions, fault management actions, and SPARC TPM management operations.
Read-Only (o)	The Read-Only (o) user role grants read-only permissions to view the state of all Oracle ILOM configuration properties and to change the account password assigned to the individual user account.
Service (s)	The Service (s) user role, when enabled, grants read and write permissions to assist Oracle service engineers if on-site service is required.
a u c r o	A combination of all these users roles (aucro), when enabled, grants read and write permissions to perform backup and restore configuration functions in Oracle ILOM.

Single Sign-On Service (Enabled by Default)

The Single Sign-On (SSO) feature in Oracle ILOM is an Oracle-proprietary protocol service that enables:

- Oracle ILOM SP web interface authenticated users to launch the KVMS applications (Oracle ILOM Remote System Console or Oracle ILOM Storage CLI Redirection) without requiring users to re-enter their passwords.
- Oracle ILOM CMM authenticated users to navigate to individual managed blade servers installed in the chassis, without requiring users to re-enter their passwords. For more information about managing blade servers from the CMM web interface or CLI, refer to the [“Getting Started With Oracle ILOM” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#).

The property state for the SSO service in Oracle ILOM is enabled by default. To modify this property state, see the following table

User Interface Configurable Target:

- **CLI:** `/SP|CMM/services/`
- **Web:** ILOM Administration > User Management > User Accounts > Single Sign On
- **Requirement:** User Management (a) role is required to modify SSO property.

Property	Default Value	Description
Single Sign On	Enabled	<i>Enabled Disabled</i>
(/sso state=)		CLI SSO State Syntax Examples Single server SP or CMM: set /SP CMM/services/sso state=enabled disabled Multi-domain server SP: As of SPARC system firmware release 9.9, use this syntax: set /SP/services/sso state=enabled disabled Prior to SPARC system firmware release 9.9, use this syntax: set /Servers/PDomains/PDomain_n/SP/services/sso state=enabled disabled

Maximum Number of User Sessions Supported

Oracle ILOM supports a maximum of 10 concurrent active user sessions for a single-server SP or CMM. Some SPARC single-server SPs are limited to a maximum of 5 concurrent active user sessions. Further, if the SPARC server is a multi-server SP, a maximum of 25 concurrent active user sessions are permitted per SP.

Note - An *active user session* is considered any of the following connections to Oracle ILOM: serial console, Secure Shell (SSH), or web interface.

To determine the maximum number of user sessions supported, click the More details... link in the ILOM Administration → User Management → User Account page in the web interface.

Manage User Authenticated Sessions per Managed Device

Using the Oracle ILOM CLI or web interface, system administrators can identify a list of users currently logged in to Oracle ILOM, as well as the type of session they initiated (web, console, or shell). System administrators can also use the CLI or web interface to terminate an active

user session in Oracle ILOM. Terminating a user session might be necessary, for example, if a user forgets to exit their session before leaving for vacation.

Note - Deleting a user account will *not* automatically terminate any active user sessions remaining in Oracle ILOM for that user.

To view an active list of users sessions or to terminate an active user session, see the following table.

User Interface Configurable Target:

- **CLI:** `/SP|CMM/sessions/`
- **Web:** **ILOM Administration > User Management > Active Sessions**
- **User Role:** **Admin (a) role is required to terminate a user session.**

Property	Description
Active Sessions (/sessions)	To view a list of users currently logged in to Oracle ILOM from the web interface, click User Management > Active Sessions. Show Active Sessions - CLI Syntax ■ From a single-server SP or a CMM, type: show /SP CMM/sessions ■ From a multi-domain server SP, type: show /Servers/PDomains/PDomain_n/SP/sessions Possible property values shown for <code>/session type= shell console web snmp video redirection serialredirection</code> ■ Shell - Active CLI session for either an SSH session or IPMI session. ■ Console - Active console session through serial console port. ■ Web - Active web browser session. ■ SNMP - Active SNMP session. ■ Video Redirection - Active host KVM redirection or active Oracle ILOM Remote System Console Plus video redirection. ■ Serial Redirection - Active host serial redirection or active Oracle ILOM Remote System Console Plus serial redirection. Possible property values shown for <code>/session mode= normal service escalation</code>
Active Session > Terminate (/sessions)	To delete an active user session from the web interface, click User Management > Sessions, then select a user session from the table and click Terminate. A confirmation message appears, click OK to continue or Cancel to cancel the action. Delete Active Session - CLI Syntax ■ From a single-server SP or a CMM, type: delete /SP CMM/sessions/n A confirmation message appears, type Y to continue or N to cancel the action.

User Interface Configurable Target:

- **CLI:** `/SP|CMM/sessions/`
- **Web:** **ILOM Administration > User Management > Active Sessions**
- **User Role:** Admin (a) role is required to terminate a user session.

Property	Description
	■ From a multi-server SP or a CMM, type: <code>delete /Servers/PDomains/PDomain_n/SP/sessions/n</code> A confirmation message appears, type Y to continue or N to cancel the action.

CLI Authentication Using Local User SSH Key

As an alternative to using a standard user password, system administrators can associate a generated public SSH key file with a user account to gain access to the Oracle ILOM CLI over a secure shell. By associating a generated public SSH key file with an Oracle ILOM account, automated scripts can execute SP commands securely in Oracle ILOM without manual intervention, or the need to embed a cleartext password.

Prior to appending a public SSH key file to an Oracle ILOM user account, you must first generate the private and public key pair using an SSH connectivity tool, like `ssh-keygen`, and store the generated SSH key files on a remote SSH system.

Note - The maximum SSH key size for RSA is 8192 bits. The SSH key size for DSA must be 1024 bits.

To upload and append a generated user public SSH key file to an Oracle ILOM user account, or to remove a user public SSH key file from an Oracle ILOM user account, see the following table.

TABLE 12 Adding or Removing Public SSH Key File per Local User Account

User Interface Configurable Target:	
■ CLI: <code>/SP CMM/users</code> ■ Web: ILOM Administration > User Management > User Accounts > SSH Key ■ User Role: Read-only (o) for personal SSH key, User Management (u) for other user SSH key	
Property	Description
Key Upload - File Transfer Options	<code>Browser TFTP SFTP SCP HTTP HTTPS Paste</code>
(set load_uri=)	For a description of each file transfer method, see Table 14, “File Transfer Methods,” on page 50.
Add SSH Key	CLI Add SSH Key Syntax:
(/ssh/keys/1)	<code>set /SP/users/user_account_name/ssh/keys/1 load_uri=transfer_method://username:password@ipaddress_or_hostname/directorypath/filename</code>

User Interface Configurable Target:

- CLI: `/SP|CMM/users`
- Web: **ILOM Administration > User Management > User Accounts > SSH Key**
- User Role: Read-only (o) for personal SSH key, User Management (u) for other user SSH key

Property	Description
	Example: <code>set /SP/users/adminuser/ssh/keys/1 load_uri=scp://adminuser:userpswd@198.51.100.4/keys/sshkey_1.pub</code> Note - The maximum SSH key size for RSA is 8192 bits. The SSH key size for DSA must be 1024 bits. The supported SSH key sizes for ECDSA are 256, 384, and 521 bits.
Delete SSH Key	CLI Delete SSH Key Syntax:
(clear action=true)	<code>set /SP CMM/users/user_account_name/ssh/keys/1 clear_action=true</code> Type y to clear public SSH Key or type n to cancel operation.
Save	Web interface only. To apply changes made to properties within the SSH Key dialog, you must click Save.

Security Action: Change Default root Account Password

To enable first-time login and access to Oracle ILOM, a default Administrator (root) 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 (root) account has since been changed, contact your system administrator for an Oracle ILOM user account with Administrator privileges.

For further details on how to modify user accounts in Oracle ILOM, see [Table 16, “View, Modify, or Remove User Account,” on page 52.](#)

Password Recovery for Default root Account

If necessary, system administrators can recover the preconfigured Oracle ILOM local root account or the password for the local root account by using the preconfigured Oracle ILOM default user account password. For further recovery instructions, see the following table.

TABLE 13 Recover Preconfigured root Account or root Account Password (CLI only)

Prerequisites	Instructions
■ Local Serial Management Connection to Oracle ILOM	1. Establish a local serial management connection to Oracle ILOM and log in to Oracle ILOM using the default user account. For example:

Prerequisites	Instructions
Physical presence at managed server, if Physical Presence State is enabled (default)	SUNSP-0000000000 login: default Press and release the physical presence button. Press return when this is completed... - Prove physical presence at your server. Refer to the server hardware documentation for instructions on how to prove physical presence. If your server hardware documentation does not mention physical presence, contact your Oracle service representative. - Return to your serial console and press Enter. You will be prompted for a password. - Type the password for the default user account: defaultpassword. - Reset the account password or re-create the root account. Refer to the Related Information section of this table for topics for creating or modifying user accounts or passwords.

Related Information

- [“Security Action: Change Default root Account Password” on page 49](#)
- [“Configure a Dedicated Local Management Connection to Oracle ILOM” on page 23](#)
- (Physical Presence) [“Assigning System Identification Information” on page 140](#)
- [“Managing Password Policy Restrictions for Local Users” on page 53](#)
- [Table 15, “Create User Account and Assign User Roles,” on page 51](#)
- [Table 16, “View, Modify, or Remove User Account,” on page 52](#)

Supported File Transfer Methods

Oracle ILOM supports the following transfer methods to upload files, such as SSH keys or security certificates, to Oracle ILOM.

TABLE 14 File Transfer Methods

File Transfer Method	Description
Browser	The Browser file transfer method is available for the web interface only. This method enables the selection of a file that is either stored locally on the system or remotely on a network share.
TFTP	The TFTP file transfer method requires you to specify the TFTP host name and the directory path to upload the designated file to Oracle ILOM.
FTP	The FTP file transfer method requires you to specify the FTP host system name, the FTP host user name and password, and then the directory path to upload the designated file.
SFTP	The SFTP file transfer method requires you to specify the SFTP host system name, the SFTP host user name and password, and then the directory path to the designated file.
SCP	The SCP file transfer method requires you to specify the SCP host system name, the SCP host user name and password, and then the directory path to the designated file.

File Transfer Method	Description
HTTP	The HTTP file transfer method requires you to specify the HTTP host system name, the HTTP user name and password, and then the directory path to the designated file.
HTTPS	The HTTPS file transfer method requires you to specify the HTTPS host system name, the HTTP host user name and password, and then the directory path to the designated file. Note - File transfer using the HTTPS protocol is not supported in Oracle ILOM firmware version 3.2.4 and earlier. This limitation in firmware releases 3.2.4 and earlier affect all file transfers using <code>dump_uri</code> or <code>load_uri</code> CLI properties, as well as selecting the HTTPS option from the Transfer Method list box in the Web interface.
Paste	The Paste file transfer method is available for the web interface only. This method provides a text box to paste in the custom certificate file.

Configuring Local User Accounts

System administrators can create and maintain up to 10 local user accounts in Oracle ILOM. For instructions for using configurable properties in Oracle ILOM to create or maintain local user accounts, see the following tables:

Note - For SPARC platforms, such as the M-series servers, system administrators can create and maintain up to 60 local user accounts. To determine the maximum number of user accounts supported, click the More details... link in the ILOM Administration → User Management → User Account page in the web interface.

- [Table 15, “Create User Account and Assign User Roles,” on page 51](#) Create User Account and Assign User Roles
- [Table 16, “View, Modify, or Remove User Account,” on page 52](#) View, Modify, or Remove User Account

Note - Deleting a user account will *not* automatically terminate any active user sessions remaining in Oracle ILOM for that user. To manage user sessions, see [“Manage User Authenticated Sessions per Managed Device” on page 46](#).

TABLE 15 Create User Account and Assign User Roles

User Interface Configurable Target:	
■ CLI: <code>/SP CMM/users/</code> ■ Web: ILOM Administration > User Management > User Accounts ■ User Role: User Management (u) (required to create user accounts).	
Property	Description
Users > Add	<code>user_name Password= Role=administrator operator advanced (a u c r o s)</code>

User Interface Configurable Target:

- **CLI:** `/SP|CMM/users/`
- **Web:** ILOM Administration > User Management > User Accounts
- **User Role:** User Management (u) (required to create user accounts).

Property	Description
<code>(user_name password= role =)</code>	Populate the Add User properties with a user name and password, then confirm the password, and assign a user role. The user name must be 4 to 16 characters and must start with an alphabetic character and use no spaces. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon and space. CLI Create User Syntax: <pre>create /SP CMM/users/user_name_for_account password= password_for_account role=administrator operator a u c r o s</pre> Example Syntax: <pre>create /SP/users user5 password=administrator role=aucr</pre> Note. When adding a user account through the CLI, it is unnecessary to provide a property value for a role or password. The role will default to Read-Only (o), and the CLI will prompt you to provide and confirm a password.
Save	Web interface – To apply changes made to properties within the Add User dialog, you must click Save.

TABLE 16 View, Modify, or Remove User Account**User Interface Configurable Target:**

- **CLI:** `/SP|CMM/users/`
- **Web:** ILOM Administration > User Management > User Accounts
- **User Role:** User Management (u) is required to modify the account of another user. Any user can modify their own password, no specific user role required.

Property	Description
Users	View local user accounts configured in Oracle ILOM.
<code>(/users)</code>	CLI View Users Syntax: <pre>show /SP CMM/users</pre> Example syntax: <pre>show /SP/users</pre>
Users > Edit	<pre>Password=user_configurable role=administrator operator advanced (a u c r o s)</pre>
<code>(/user_name password= role=)</code>	Edit the applicable User properties for password and user role. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon and space. Note that the user roles cannot be modified for the preconfigured root user. Web interface – Click Save to apply the changes made within the Edit User dialog. CLI Edit User Account Syntax:

User Interface Configurable Target:

- CLI: `/SP|CMM/users/`
- Web: ILOM Administration > User Management > User Accounts
- User Role: User Management (u) is required to modify the account of another user. Any user can modify their own password, no specific user role required.

Property	Description
	set <code>/SP CMM/users user_name password=assign_new_password role=administrator operator a u c r o s</code> Example Syntax: <code>set /SP/users user5 password=administrator role=auco</code>
Users > Delete (/user_name)	Specify the name of the user account to delete. When prompted, confirm the action. Note - Deleting a user account will <i>not</i> automatically terminate any active user sessions remaining in Oracle ILOM for that user. To manage user sessions, see “Manage User Authenticated Sessions per Managed Device” on page 46 . CLI Delete User Account Syntax: delete <code>/SP CMM/users/user_name</code> Example Syntax: <code>delete /SP/users/user5</code>

Related Information

- [“Managing Password Policy Restrictions for Local Users” on page 53](#)
- [Table 10, “ Privileges Granted by a User Profile,” on page 44](#)
- [Table 16, “ View, Modify, or Remove User Account,” on page 52](#)
- [Table 6, “Local User Accounts Enabled by Default,” on page 38](#)
- [Table 13, “Recover Preconfigured root Account or root Account Password \(CLI only\),” on page 49](#)
- [“CLI Authentication Using Local User SSH Key ” on page 48](#)
- [“Security Action: Change Default root Account Password” on page 49](#)
- [Table 15, “Create User Account and Assign User Roles,” on page 51](#)

Managing Password Policy Restrictions for Local Users

Oracle ILOM, as of firmware release 3.2.5, enforces a password policy for all local user accounts. The password policy ships with a default set of password policy restrictions. System administrators can either choose to use the default properties as is or modify them to meet their password policy needs.

Note - Modifications to the password policy properties should be set prior to creating local user accounts. In the event that the Password Policy properties are modified after configuring local user accounts, Oracle ILOM will automatically: 1) remove the configuration of all local user accounts, and 2) restore the default root account that was initially provided with the system.

Oracle ILOM automatically enforces all configured password policy restrictions whenever local user account passwords are changed or created.

For further details about modifying the default password policy restrictions provided, see the following sections:

- [“Modify Password Policy Restrictions for Local Users” on page 54](#)
- [“Password Policy Management Properties and Defaults” on page 57](#)

▼ Modify Password Policy Restrictions for Local Users

Before You Begin

- The Admin (a) role is required to configure the Password Policy properties.
- The Password Policy applies only to local user accounts. It has no impact on remote user authentication service accounts like LDAP or Active Directory.
- The Password Minimum Length property, by default, is set to eight characters. When the minimum length is set to less than eight characters, the password policy is considered weak. To ensure greater security, set the minimum password length value from eight to sixteen characters.
- Upon saving changes to the password policy properties, the following will occur:
 - All local user account configurations are deleted from Oracle ILOM.
 - The default local user account (root) shipped with the system is restored.
 - On the initial log in of root, the root user is prompted to change the root-account-password.

Follow these steps to set a password policy for all local user accounts.

1. View the current Password Policy properties in Oracle ILOM:

- **Web:** Click ILOM Administration > User Management > Password Policy.
- **CLI:** Type the following command string:

`show /SP/preferences/password_policy`

2. Modify, as required, the applicable Password Policy properties:

■ **Web: Perform the following steps:**

- a. **In the Minimum Length text box, if necessary, modify the default value of eight password characters.**

Note - The minimum password length can be set from 1 to 16 characters depending on the needs of your organization. However, when greater security is required, the Minimum Length property should always be set to a value from 8 to 16 characters.

- b. **Configure the Password Policy check box properties as required.**

To enable a check box property, select the check box. To disable a check box property, clear the check box.

For a description of each Password Policy property, see [Table 17, “Management Properties for Password Policy,” on page 57.](#)

- c. **Click Save to save the changes.**

- If the Minimum Length property is set to eight or more characters. The following message appears:

Clicking 'OK' will cause all user accounts to be deleted and restored to factory defaults. Click 'Cancel' to not change the password policy and keep current user accounts.

-or-

- If the Minimum Length property is set to less than eight characters The following messages appear:

Warning: A password length less than 8 is considered weak. Do you want to continue?

If you click OK to continue, the following message appears:

Clicking 'OK' will cause all user accounts to be deleted and restored to factory defaults. Click 'Cancel' to not change the password policy and keep current user accounts.

- d. **Click OK to continue saving your changes and to update the password policy restrictions; otherwise, click Cancel.**

If you click OK, all user-defined local account configurations are deleted and the default root account is restored to its default password.

■ **CLI: Perform the following steps:**

a. **Type the following command string:**

```
set /SP/preferences/password_policy/policy=[min_length].[restrictions]
```

where:

- *min_length* = Minimum password length of 1 to 16 characters. (Required)

Note - The Password Minimum Length property, by default, is set to eight characters. When the minimum length is set to less than eight characters, the password policy is considered weak. To ensure greater security, set the minimum password length value from eight to sixteen characters.

- *.* = A separator (*period*) following the minimum length value (*Required*)
- *restrictions* = One or more of the following characters:
 - *u* = at least one uppercase letter is required in password (*Optional*)
 - *l* = at least one lowercase letter is required in password (*Optional*)
 - *n* = at least one number is required in password (*Optional*)
 - *s* = at least one symbol is required in password (*Optional*)
 - *h* = password history check is enabled (*Optional*)

Example:

To set the password policy properties for maximum length of 10 and to require at least one uppercase letter and number, you would type:

```
set /SP/preferences/password_policy/policy=10.un
```

For a description of each password policy property, see [Table 17, “Management Properties for Password Policy,” on page 57](#).

b. **Press Enter.**

- If the Minimum Length property is set to eight or more characters. The following message appears:

```
All user accounts will be deleted. The system will restore factory
default users. Do you want to continue (y/n)?
```

-or-

- If the Minimum Length property is set to less than eight characters The following messages appear:

Warning: a password length less than 8 is considered weak. Do you want to continue (y/n)? y

If you type y to continue, the following message appears:

All user accounts will be deleted. The system will restore factory default users. Do you want to continue (y/n)?

- c. **Type y to save the updated password policy restrictions; otherwise, type n to cancel the changes.**

If you type y, all user-defined local account configurations are deleted and the default root account is restored to its default password.

Related Information:

- [“Securing Oracle ILOM User Access” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x](#)
- [“Post Deployment Considerations for Securing User Access” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x](#)
- [“Security Action: Change Default root Account Password” on page 49](#)
- [“Password Recovery for Default root Account” on page 49](#)
- [“Configuring Local User Accounts ” on page 51](#)

Password Policy Management Properties and Defaults

The following table describes the CLI and web properties for the Oracle ILOM Password Policy feature.

TABLE 17 Management Properties for Password Policy

Property	Default	Description
Minimum Length (1-16)	8	Any value from 1 to 16 The Minimum Length property defines the minimum number of characters that a local user account password must contain to be policy compliant. Note - A password minimum length that is set to less than eight characters is considered a weak password policy.
Uppercase Letters	Disabled, no restrictions	Disabled (no restrictions) Enabled (requires at least 1),

Property	Default	Description
(u)		The Uppercase Letters property controls whether a local user account password must contain at least one uppercase letter to be policy compliant. By default, Oracle ILOM does not require the use of an uppercase letter in the local user account password. System administrators can enforce local users to include at least one uppercase letter in their password by enabling the Uppercase Letters property.
Lowercase Letters (l)	Disabled, no restrictions	Disabled (no restrictions) Enabled (requires at least 1) The Lowercase Letters property controls whether a local user account password must contain at least one lowercase letter to be policy compliant. By default, Oracle ILOM does not require the use of a lowercase letter in the local user account password. System administrators can enforce local users to include at least one lowercase letter in their password by enabling the Lowercase Letters property.
Numbers (n)	Disabled, no restrictions	Disabled (no restrictions) Enabled (requires at least 1) The Numbers property controls whether a local user account password must contain at least one numeric character to be policy compliant. By default, Oracle ILOM does not require the use of a numeric character in the local user account password. System administrators can enforce local users to include at least one numeric character in their password by enabling the Numbers property.
Symbols (s)	Disabled, no restrictions	Disabled (no restrictions) Enabled (requires at least 1) Symbols permitted include: ! @ # \$ % ^ & * () The Symbols property controls whether a local user account password must contain at least one symbol character to be policy compliant. By default, Oracle ILOM does not require the use of a symbol in the local user account password. System administrators can enforce local users to include at least one symbol character in their password by enabling the Symbols property. Note - Extended ASCII symbols and colons (:) are not acceptable password characters.
History (h)	Disabled, no restrictions	Disabled (no restrictions) Enabled (cannot use 5 previous passwords). The History property controls whether Oracle ILOM prevents local users from using their last five passwords. By default, Oracle ILOM does not restrict local users from reusing any of their last five passwords. System administrators can prevent local users from reusing their previous passwords by enabling the History property.

Configuring Active Directory

System administrators can optionally configure Oracle ILOM to use the Microsoft Windows Active Directory service to authenticate Oracle ILOM users, as well as define user authorization levels for using the features within Oracle ILOM. This service is based on a client-server query model that uses the assigned user password to authenticate Active Directory users.

The property for the Active Directory service state, in Oracle ILOM, is disabled by default. To enable the Active Directory service state and configure Oracle ILOM as an Active Directory client, see the following tables:

- [Table 18, “Enabling Active Directory Authentication,” on page 59](#) Enabling Active Directory Authentication
- [Table 19, “Uploading or Removing an Active Directory Certificate File,” on page 63](#) Uploading or Removing an Active Directory Certificate File
- [Table 20, “Optionally Configuring Active Directory Groups,” on page 64](#) Optionally Configuring Active Directory Groups
- [Table 21, “Configuring Active Directory User Domains,” on page 67](#) Configuring Active Directory User Domains
- [Table 22, “Optionally Configuring Active Directory Alternate Servers,” on page 67](#) Optionally Configuring Active Directory Alternate Servers
- [Table 23, “Optionally Editing DNS Locator Queries,” on page 68](#) Optionally Editing DNS Locator Queries
- [Table 24, “Guidelines for Troubleshooting Active Directory Authentication,” on page 69](#) Guidelines for Troubleshooting Active Directory Authentication

TABLE 18 Enabling Active Directory Authentication

User Interface Configurable Target:		
■ CLI: <code>/SP CMM/clients/activedirectory</code> ■ Web: ILOM Administration > User Management > Active Directory > Settings ■ User Role: User Management (u) (required for all property modifications) ■ Prerequisite: The Active Directory server must be configured with users or user groups prior to configuring Oracle ILOM as an Active Directory client.		
Property	Default Value	Description
State	Disabled	<i>Disabled Enabled</i>
(state=)		To configure Oracle ILOM as an Active Directory client, set the State property to enabled. When the State property is enabled, and the Strict Certificate Mode property is disabled, Oracle ILOM over a secure channel provides some validation of the Active Directory service certificate at the time of user authentication. When the State property is enabled, and the Strict Certificate Mode property is enabled, Oracle ILOM over a secure channel fully verifies the Active Directory service certificate for digital signatures at the time of user authentication.

User Interface Configurable Target:

- **CLI:** `/SP|CMM/clients/activedirectory`
- **Web:** ILOM Administration > User Management > Active Directory > Settings
- **User Role:** User Management (u) (required for all property modifications)
- **Prerequisite:** The Active Directory server must be configured with users or user groups prior to configuring Oracle ILOM as an Active Directory client.

Property	Default Value	Description
CLI State Syntax:		
set /SP CMM/clients/activedirectory/ state=disabled enabled		
Roles (defaultrole=)	None (server authorization)	<i>Administrator Operator Advanced None (server authorization)</i> To define which features in Oracle ILOM are accessible to Active Directory authenticated users, set the default Role property to one of the four property values accepted: Administrator (a u c r o), Operator (c r o), Advanced (a u c r o s), or None (server authorization). When the Default Role property is set to an Oracle ILOM user role, authorization levels for using features within Oracle ILOM are dictated by the privileges granted by the configured Oracle ILOM user role. For a description of privileges assigned, see the user role and user profile topics listed in the Related Information section below. When the Role property is set to None (server authorization), and Oracle ILOM is configured to use Active Directory Groups, the authorization levels for using features within Oracle ILOM are dictated by the Active Directory Group. For further configuration details, see the Active Directory Group topic listed in the Related Information section below. CLI Roles Syntax: set /SP CMM/clients/activedirectory/ defaultrole=adminstrator operator a u c r o s none Related Information: ■ Table 10, “Privileges Granted by a User Profile,” on page 44 ■ Table 10, “Privileges Granted by a User Profile,” on page 44 ■ Table 20, “Optionally Configuring Active Directory Groups,” on page 64
Address (address=)	0.0.0.0	<i>IP address DNS host name (Active Directory Server)</i> To configure the Active Directory server network address, populate the Address property with the Active Directory server IP address or DNS host name. If a DNS host name is used, then the DNS configuration properties in Oracle ILOM must be properly configured and operational. CLI Address Syntax: set /SP CMM/clients/activedirectory/ address=active_directory_server ip_address active_directory_server_dns_host_name Related Information: ■ Table 48, “DNS Configuration Properties ,” on page 134
Port	0 (Auto-select)	<i>0 Auto-select Non-standard TCP port</i>

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/activedirectory`
- Web: ILOM Administration > User Management > Active Directory > Settings
- User Role: User Management (u) (required for all property modifications)
- Prerequisite: The Active Directory server must be configured with users or user groups prior to configuring Oracle ILOM as an Active Directory client.

Property	Default Value	Description
(port=)		A standard TCP port is used by Oracle ILOM to communicate with the Active Directory server. When the Port Auto-select property is enabled, the Port number is set to 0 by default. When the Port Auto-select property is disabled, the Port number property in the web interface becomes user-configurable. A configurable Port property is provided in the unlikely event of Oracle ILOM needing to use a non-standard TCP port. CLI Port Syntax: set /SP CMM/clients/activedirectory/ port=number
Timeout (timeout=)	4 seconds	4 user-specified The Timeout property designates the number of seconds to wait for an individual transaction to complete. The value does not represent the total time for all transactions to complete since the number of transactions can differ depending on the configuration. The Timeout property is set to 4 seconds by default. If necessary, adjust this property value as needed to fine tune the response time for when the Active Directory server is unreachable or not responding. CLI Timeout Syntax: set /SP CMM/clients/activedirectory/ timeout=number_of_seconds
Strict Certificate Mode (strictcertmode=)	Disabled	Disabled Enabled When the Strict Certificate Mode property is enabled, Oracle ILOM fully verifies the digital signatures in the Active Directory certificate at the time of authentication. When the Strict Certificate Mode property is disabled, Oracle ILOM provides limited validation of the server certificate at the time of authentication over a secure channel. Caution - The Active Directory server certificate must be loaded prior to enabling the Strict Certificate Mode property. CLI Strict Certificate Mode Syntax: set /SP CMM/clients/activedirectory/ strictcertmode=disabled enabled Related Information: ■ Table 19, “Uploading or Removing an Active Directory Certificate File,” on page 63
DNS Locator Mode (/dnslocatorqueries)	Disabled	Disabled Enabled To configure Oracle ILOM to use DNS Locator Queries to obtain a list of Active Directory servers, set the DNS Locator Mode property to enabled.

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/activedirectory`
- Web: ILOM Administration > User Management > Active Directory > Settings
- User Role: User Management (u) (required for all property modifications)
- Prerequisite: The Active Directory server must be configured with users or user groups prior to configuring Oracle ILOM as an Active Directory client.

Property	Default Value	Description
		CLI DNS Locator Mode Syntax: set /SP CMM/clients/activedirectory/dnslocatorqueries/1=disabled enabled Related Information: ■ Table 23, “Optionally Editing DNS Locator Queries,” on page 68
Expanded Search Mode (expsearchmode=)	Disabled	<i>Disabled Enabled</i> To configure Oracle ILOM to use additional search options for locating Active Directory user entries, set the Expanded Search Mode property to enabled. When the Expanded Search Mode property is disabled, Oracle ILOM will use the userPrincipleName to search for user entries. In which case, the userPrincipleName must have a fully qualified domain name (FQDN) suffix. CLI Expanded Search Mode Syntax: set /SP CMM/clients/activedirectory/ expsearchmode=disabled enabled
Strict Credential Error Mode (strictcredentialerrormode=)	Disabled	<i>Disabled Enabled</i> When the Strict Credential Error Mode property is enabled, and user credential errors are reported from any server, Oracle ILOM fails those user credentials. When the Strict Credential Error Mode property is disabled, Oracle ILOM presents the user credential to other Active Directory servers for authentication (configured as alternate servers or found by DNS Locator Queries). CLI Strict Credential Error Mode Syntax: set /SP CMM/clients/activedirectory/ strictcredentialerrormode=disabled enabled Related Information: ■ Table 19, “Uploading or Removing an Active Directory Certificate File,” on page 63
Log Detail (logdetail=)	None	<i>None High Medium Low Trace</i> To specify the amount of diagnostic information recorded in the Oracle ILOM event log for Active Directory events, set the Log Detail property to one of the accepted property values. CLI Log Detail Configuration Syntax:

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/activedirectory`
- Web: ILOM Administration > User Management > Active Directory > Settings
- User Role: User Management (u) (required for all property modifications)
- Prerequisite: The Active Directory server must be configured with users or user groups prior to configuring Oracle ILOM as an Active Directory client.

Property	Default Value	Description
		set <code>/SP CMM/clients/activedirectory/logdetail=none high medium low trace</code>
Save		Web interface – To apply changes made to properties within the Active Directory Settings page, you must click Save.

TABLE 19 Uploading or Removing an Active Directory Certificate File**User Interface Configurable Target:**

- CLI: `/SP|CMM/clients/activedirectory/cert`
- Web: ILOM Administration > User Management > Active Directory > Certificate Information
- User Role: (u) User Management (required for all property modifications)

Property	Default Value	Description
Certificate File Status (certstatus=)	Read-only	<i>Certificate present Certificate not present</i> The Certificate File Status property indicates whether an Active Directory certificate has been uploaded to Oracle ILOM. Caution - The Active Directory certificate file must be uploaded to Oracle ILOM prior to enabling the Strict Certificate Mode property. CLI Certificate Show Syntax: show <code>/SP CMM/clients/activedirectory/cert</code>
File Transfer Method	Browser (web interface only)	<i>Browser TFTP FTP SCP Paste</i> For a detailed description of each file transfer method, see Table 14, “File Transfer Methods,” on page 50.
Load Certificate (load_uri=)		Web interface – Click the Load Certificate button to upload the Active Directory Certificate file that is defined in the File Transfer Method properties. CLI Certificate Load Syntax: load_uri=<i>file_transfer_method://host_address/file_path/filename</i>
Remove Certificate (clear_action=true)		Web interface – Click the Remove Certificate Button to remove the Active Directory Certificate file presently stored in Oracle ILOM. When prompted, type y (Yes) to delete or n (No) to cancel the action. CLI Remove Certificate Syntax: set <code>/SP CMM/clients/activedirectory/cert clear_action=true</code> -or-

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/activedirectory/cert`
- Web: ILOM Administration > User Management > Active Directory > Certificate Information
- User Role: (u) User Management (required for all property modifications)

Property	Default Value	Description
		reset <code>/SP CMM/clients/activedirectory/cert</code>
		When prompted, type y to delete or n to cancel the action.

TABLE 20 Optionally Configuring Active Directory Groups**User Interface Configurable Target:**

- CLI: `/SP|CMM/clients/activedirectory`
- Web: ILOM Administration > User Management > Active Directory > (Name) Groups
- User Role: (u) User Management (required for all property modifications)
- Prerequisite: Prior to setting up Activity Directory Groups in Oracle ILOM, the Active Directory Groups must be present on the Active Directory server and assigned members.

Property	Description
Admin Groups (/admingroups/1 2 3 4 5)	A system administrator can optionally configure Admin Group properties instead of the Role properties in Oracle ILOM to provide user authorization. Oracle ILOM supports the configuration of up to five Admin Groups. When Admin Group properties are enabled in Oracle ILOM, a user's group membership is checked for any matching groups defined in the admin table. If a match occurs, the user is granted Administrator-level access. Note – Oracle ILOM grants a group member one or more authorization levels based on the matching groups (Operator, Administrator, or Custom) found in each configured group table. Use the following possible values to populate the configuration properties for each Active Directory Admin Group in Oracle ILOM: ■ DN format: CN=admingroup,OU=groups,DC=domain,DC=company,DC=com ■ NT Domain format: domain\admingroup ■ Full Domain format: DC=domain,DC=company,DC=com\admingroup ■ Simple Name format: admingroup (Up to 128 characters) CLI Configuration Syntax for Admin Groups: set <code>/SP CMM/clients/activedirectory/admingroups/n name=string</code> Example Syntax: <pre>set /SP/clients/activedirectory/admingroups/1/ name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com</pre> Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com'
Operator Groups (/operatorgroups/1 2 3 4 5)	A system administrator can optionally configure Operator Group properties instead of the Role properties in Oracle ILOM to provide user authorization.

User Interface Configurable Target:

- **CLI:** `/SP|CMM/clients/activedirectory`
- **Web:** **ILOM Administration > User Management > Active Directory > (Name) Groups**
- **User Role:** (u) User Management (required for all property modifications)
- **Prerequisite:** Prior to setting up Active Directory Groups in Oracle ILOM, the Active Directory Groups must be present on the Active Directory server and assigned members.

Property	Description
	Oracle ILOM supports the configuration of up to five Operator Groups. When Operator Group properties are enabled in Oracle ILOM, a user's group membership is checked for any matching groups defined in the operator table. If a match occurs, the user is granted Operator-level access. Note – Oracle ILOM grants a group member one or more authorization levels based on the matching groups (Operator, Administrator, or Custom) found in each configured group table. Use the following possible values to populate the configuration properties for each Operator Group in Oracle ILOM: ■ DN format: CN=operatorgroup,OU=groups,DC=domain,DC=company,DC=com ■ NT Domain format: domain\operatorgroup ■ Full Domain format: DC=domain,DC=company,DC=com\operatorgroup ■ Simple Name format: operatorgroup (Up to 128 characters) CLI Configuration Syntax for Operator Groups: <pre>set /SP CMM/clients/activedirectory/operatorgroups/n name=string</pre> Example Syntax: <pre>set /SP/clients/activedirectory/operatorgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com</pre> Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com''
Host Groups	Active Directory Host Groups properties are specific to Oracle's multi-domain SPARC server systems. For multi-domain SP server systems, Oracle ILOM enables system administrators to configure up to 10 host groups for Active Directory user authentication. CLI Configuration Syntax for Host Groups: <pre>set /SP/clients/activedirectory/hostgroups/n/ name=string hosts=string roles=string</pre> Where: ■ name= is a read and write property that represents the Active Directory group name for the specified host group. ■ hosts= is a read and write property that lists the PDomain for which this host group assigns roles. ■ roles= is a read/write property that specifies the domain-specific privilege levels for the host group. This property supports any of the individual host role ID combinations of a, c, and r (for example, acr) where a= admin, c=console, and r=reset.

User Interface Configurable Target:

- **CLI:** `/SP|CMM/clients/activedirectory`
- **Web:** ILOM Administration > User Management > Active Directory > (Name) Groups
- **User Role:** (u) User Management (required for all property modifications)
- **Prerequisite:** Prior to setting up Activity Directory Groups in Oracle ILOM, the Active Directory Groups must be present on the Active Directory server and assigned members.

Property	Description
	For further details about configuring Host Group properties for multi-domain server SP systems, see the administration guide available for the Oracle server.
Custom Groups (/customgroups/1 2 3 4 5)	A system administrator can optionally configure up to five Custom Group properties in Oracle ILOM to provide user authorization. Oracle ILOM uses the Custom Group properties to determine the appropriate user roles to assign when authenticating users who are members of a Custom Group. When enabling the use of Custom Groups in Oracle ILOM, both the Roles property and the Custom Groups property must be configured. For further information about the configuration properties for Roles, see the Roles property in Table 18, “Enabling Active Directory Authentication,” on page 59. Note – Oracle ILOM grants a group member one or more authorization levels based on the matching groups (Operator, Administrator, or Custom) found in each configured group table. Use the following possible values to populate the configuration properties for each Custom Group in Oracle ILOM: ■ User role: <i>administrator operator advanced</i> (a u c r o s) ■ DN format: CN=customgroup,OU=groups,DC=domain,DC=company,DC=com ■ NT Domain format: domain\customgroup ■ Full Domain format: DC=domain,DC=company,DC=com\customgroup ■ Simple Name format: customgroup (Up to 128 characters) CLI Configuration Syntax for Custom Groups: <pre>set /SP CMM/clients/activedirectory/customgroups/n name=string roles=administrator operator a u c r o s</pre> Example Syntax: <pre>set /SP/clients/activedirectory/customgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com roles=au</pre> Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com' roles' to 'au' Related Information: ■ “Assignable Oracle ILOM User Roles” on page 43
Save	Web interface – To apply changes made to properties in the Admin, Operator, or Custom Group dialogs, you must click Save.

TABLE 21 Configuring Active Directory User Domains

User Interface Configurable Target:	
■ CLI: <code>/SP CMM/clients/activedirectory/userdomains/n</code> ■ Web: ILOM Administration > User Management > Active Directory > User Domains ■ User Role: User Management (u) (required for all property modifications) ■ Prerequisite: Prior to setting up Activity Directory User Domains in Oracle ILOM, the Active Directory User Domains must be present on the Active Directory server and assigned members.	
Property	Description
User Domains (1 2 3 4 5)	A system administrator can optionally configure up to five User Domains. When one or more user domains are defined, Oracle ILOM uses these properties in sequence until it is able to authenticate the Active Directory user. Use the following possible values to populate configuration properties for each User Domain in Oracle ILOM: ■ UPN format: <code><USERNAME>@domain.company.com</code> ■ DN format: <code>CN=<USERNAME>,CN=Users,DC=domain,DC=company,DC=com</code> Note - You can use <code><USERNAME></code> as a literal. When <code><USERNAME></code> is used as a literal Oracle ILOM replaces the <code><USERNAME></code> during user authentication with the current login name entered. CLI User Domains Syntax: <pre>set /SP CMM/clients/activedirectory/userdomains/n name=string</pre> Example 1: <code>name=CN=<USERNAME></code> <pre>set /SP/clients/activedirectory/userdomains/1/name=CN<USERNAME>, OU=Groups, DC=sales, DC-Oracle, DC=com</pre> Set 'name' to 'CN=<USERNAME>,OU=Groups,DC=sales,DC=oracle,DC=com' Example 2: <code>name=CN=spSuperAdmin</code> <pre>set /SP/clients/activedirectory/userdomains/1/ name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com</pre> Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com'
Save	Web interface – To apply changes made to properties in the Active Directory User Domains dialog, you must click Save.

TABLE 22 Optionally Configuring Active Directory Alternate Servers

User Interface Configurable Target:	
■ CLI: <code>/SP CMM/clients/activedirectory/alternateservers/n</code> ■ Web: ILOM Administration > User Management > Active Directory > Alternate Servers ■ User Role: User Management (u) (required for all property modifications)	
Property	Description
Alternate Servers	Oracle ILOM enables a system administrator to configure up to five Active Directory alternate servers.

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/activedirectory/alternateservers/n`
- Web: ILOM Administration > User Management > Active Directory > Alternate Servers
- User Role: User Management (u) (required for all property modifications)

Property	Description
(/1 2 3 4 5)	Alternate servers provide authentication redundancy, as well as a choice of different Active Directory servers to use when you need to isolate domains. Each Active Directory alternate server uses the same user authorization rules and requirements as the primary Active Directory server. For example, Oracle ILOM will use the configured user roles in the Roles property to authenticate users. However, if the Roles property is not configured, Oracle ILOM will query the authentication server for the appropriate authorization roles. Each Active Directory alternate server has its own properties for network address, port, certificate status, and commands for uploading and removing a certificate. When an Active Directory certificate is not supplied, but is required, Oracle ILOM will use the top-level primary Active Directory server certificate. Note - If the alternate servers are being used to provide authentication redundancy, the property for Strict Credential Error Mode can be optionally enabled. However, if the alternate servers are being used to span disjoint domains, then the property for Strict Credential Error Mode should be disabled. For configuration properties for Strict Credential Error Mode, see Table 18, “Enabling Active Directory Authentication,” on page 59. CLI Alternate Server Address and Port syntax: <pre>set /SP CMM/clients/activedirectory/alternateservers/n address=string port=string</pre> CLI Alternate Server Certificate Syntax: <pre>show /SP CMM/clients/activedirectory/alternateservers/n/cert</pre> <pre>load_uri=file_transfer_method://host_address/file_path/filename</pre> <pre>set /SP CMM/clients/activedirectory/alternateservers/n/cert clear_action=true</pre>
Save	Web interface – To apply changes made to properties in the Active Directory Alternate Servers dialog, you must click Save.

TABLE 23 Optionally Editing DNS Locator Queries**User Interface Configurable Target:**

- CLI: `/SP|CMM/clients/activedirectory/dnslocatorqueries`
- Web: ILOM Administration > User Management > Active Directory > DNS Locator Queries
- User Role: User Management (u) (required for all property modifications)

Property	Default Value	Description
DNS Locator Queries	<code>_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269></code>	Oracle ILOM enables you to configure up to five DNS Locator Queries.
(/1)		A DNS locator query identifies the named DNS service and the port ID. The port ID is generally part of the record, but you can override it by using the format <code><PORT:636></code> . Additionally, you can override the named DNS service for a specific domain by using the <code><DOMAIN></code> substitution marker.
DNS Locator Queries	<code>_ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636></code>	

CLI Show and Edit DNS Locator Queries Syntax:

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/activedirectory/dnslocatorqueries`
- Web: ILOM Administration > User Management > Active Directory > DNS Locator Queries
- User Role: User Management (u) (required for all property modifications)

Property	Default Value	Description
(/2)		show <code>/SP CMM/clients/activedirectory/dnslocatorqueries/1</code> set <code>/SP CMM/clients/activedirectory/dnslocatorqueries/1</code> service = <i>string</i> Example DNS Locator Queries Syntax for service= string : <code>service = _ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:nnnn></code>
Save		Web interface – To apply changes made to properties in the Active Directory DNS Locator Queries dialog, you must click Save.

TABLE 24 Guidelines for Troubleshooting Active Directory Authentication

Refer to the following guidelines when troubleshooting Active Directory authentication and authorization attempts in Oracle ILOM.

- To test and diagnose Active Directory authentication, follow these steps:
 - 1: Set the Active Directory Log Details property to trace.
 - 2: Attempt an authentication to Oracle ILOM to generate events.
 - 3: Review the Oracle ILOM event log file.
 - Ensure that the user groups and user domains configured on the Active Directory server match the user groups and user domains configured in Oracle ILOM.
 - The Oracle ILOM Active Directory Client does not manage clock settings. The clock settings in Oracle ILOM are configurable manually or through an NTP server.
- Note.** When the clock settings in Oracle ILOM are configured using an NTP server, Oracle ILOM performs an ntpdate using the NTP server(s) before starting the NTP daemon.

Related Information:

- [Table 18, “Enabling Active Directory Authentication,” on page 59](#)
- [“Managing Oracle ILOM Log Entries” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Setting ILOM Clock Properties” on page 142](#)

Configuring LDAP/SSL

System administrators can optionally configure Oracle ILOM to use the LDAP/SSL directory service to authenticate Oracle ILOM users, as well as define user authorization levels for using features within Oracle ILOM.

The property for the LDAP/SSL service state, in Oracle ILOM, is disabled by default. To enable the LDAP/SSL service state and configure Oracle ILOM as an LDAP/SSL client, see the following tables:

- [Table 25, “Enabling LDAP/SSL Authentication ,” on page 70](#) Enabling LDAP/SSL Authentication
- [Table 26, “ Uploading or Removing an LDAP/SSL Certificate File,” on page 73](#) Uploading or Removing an LDAP/SSL Certificate File
- [Table 27, “Optionally Configuring LDAP/SSL Groups,” on page 74](#) Optionally Configuring LDAP/SSL Groups
- [Table 28, “ Configuring LDAP/SSL User Domains,” on page 76](#) Configuring LDAP/SSL User Domains
- [Table 29, “ Optionally Configuring LDAP/SSL Alternate Servers,” on page 77](#) Optionally Configuring LDAP/SSL Alternate Servers
- [Table 30, “ Guidelines for Troubleshooting LDAP/SSL Authentication,” on page 78](#) Guidelines for Troubleshooting LDAP/SSL Authentication

TABLE 25 Enabling LDAP/SSL Authentication

User Interface Configurable Target:		
■ CLI: <code>/SP CMM/clients/ldapssl/</code> ■ Web: ILOM Administration > User Management > LDAP/SSL > Settings ■ User Role: User Management (u) (required for all property modifications) ■ Prerequisite: LDAP/SSL server must be configured with users or user groups prior to configuring Oracle ILOM.		
Property	Default Value	Description
State (state=)	Disabled	<i>Disabled Enabled</i> To configure Oracle ILOM to use the LDAP/SSL authentication and authorization directory service, set the State property to enabled. When the State property is set to disabled, Oracle ILOM is disabled from using the LDAP/SSL service for user authentication and authorization levels. When the State property is enabled, and the Strict Certificate Mode property is disabled, Oracle ILOM over a secure channel provides some validation of the LDAP/SSL service certificate at the time of user authentication. When the State property is enabled, and the Strict Certificate Mode property is enabled, Oracle ILOM over a secure channel fully verifies the LDAP/SSL service certificate for digital signatures at the time of user authentication. CLI State Syntax: set <code>/SP CMM/clients/ldapssl/ state=disabled enabled</code>
Roles (defaultrole=)	None (server authorization)	<i>Administrator Operator Advanced None</i> (server authorization)

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/ldapssl/`
- Web: **ILOM Administration > User Management > LDAP/SSL > Settings**
- User Role: **User Management (u)** (required for all property modifications)
- Prerequisite: **LDAP/SSL server must be configured with users or user groups prior to configuring Oracle ILOM.**

Property	Default Value	Description
		To define which features in Oracle ILOM are accessible to LDAP/SSL authenticated users, set the default Roles property to one of the four property values accepted: Administrator (a u c r o), Operator (c r o), Advanced (a u c r o s), or None (server authorization). When the default Roles property is set to an Oracle ILOM user role, authorization levels for using features within Oracle ILOM are dictated by the user privileges granted by the Oracle ILOM user role. For a description of privileges assigned, see the tables listed in the Related Information section below for user role and user profile. When the default Roles property is set to None (server authorization) and Oracle ILOM is configured to use LDAP/SSL Groups, the authorization levels for using features within Oracle ILOM are dictated by the LDAP/SSL Group. For further LDAP/SSL configuration details, see the table that describes LDAP/SSL Groups listed in the Related Information section below. CLI Roles Syntax: <pre>set /SP CMM/clients/ldapssl/ defaultrole=admin operator a u c r o s none</pre> Related Information: ■ Table 10, “Privileges Granted by a User Profile,” on page 44 ■ Table 11, “Privileges Granted by Individual User Roles,” on page 45 ■ Table 27, “Optionally Configuring LDAP/SSL Groups,” on page 74
Address (address=)	0.0.0.0	<i>IP address DNS host name</i> (Active Directory Server) To configure the network address for the LDAP/SSL server, populate the Address property with the LDAP/SSL IP address or DNS host name. If a DNS host name is used, then the DNS configuration properties in Oracle ILOM must be properly configured and operational. CLI Address Syntax: <pre>set /SP CMM/clients/ldapssl/ address=LDAP/SSL_server ip_address active_directory_server_dns_host_name</pre> Related Information: ■ Table 48, “DNS Configuration Properties ,” on page 134
Port (port=)	0 Auto-select	<i>0 Auto-select Non-standard TCP port</i> A standard TCP port is used by Oracle ILOM to communicate with the LDAP/SSL server. When the Port Auto-select property is enabled, the Port number is set to 0 by default. When the Port Auto-select property is disabled, the Port number property in the web interface becomes user-configurable.

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/ldapssl/`
- Web: ILOM Administration > User Management > LDAP/SSL > Settings
- User Role: User Management (u) (required for all property modifications)
- Prerequisite: LDAP/SSL server must be configured with users or user groups prior to configuring Oracle ILOM.

Property	Default Value	Description
		A configurable Port property is provided in the unlikely event of Oracle ILOM needing to use a non-standard TCP port. CLI Port Syntax: set <code>/SP CMM/clients/ldapssl/ port=number</code>
Timeout (timeout=)	4 seconds	<i>4 user-specified</i> The Timeout property is set to 4 seconds by default. If necessary, adjust this property value to fine tune response time when the LDAP/SSL server is unreachable or not responding. The Timeout property designates the number of seconds to wait for an individual transaction to complete. The value does not represent the total time for all transactions to complete since the number of transactions can differ depending on the configuration. CLI Timeout Syntax: set <code>/SP CMM/clients/ldapssl/ timeout=number_of_seconds</code>
Strict Certificate Mode (strictcert mode=)	Disabled	<i>Disabled Enabled</i> When enabled, Oracle ILOM fully verifies the LDAP/SSL certificate signatures at the time of authentication over a secure channel. When disabled, Oracle ILOM provides limited validation of the server certificate at time of authentication over a secure channel. Caution - The LDAP/SSL server certificate must be uploaded to Oracle ILOM prior to enabling the Strict Certificate Mode property. CLI Strict Certificate Mode Syntax: set <code>/SP CMM/clients/ldapssl/ strictcertmode=disabled enabled</code> Related Information: ■ Table 26, “Uploading or Removing an LDAP/SSL Certificate File,” on page 73
Optional User Mapping (/optionalUsermapping)	Disabled	<i>Disabled Enabled</i> The Optional User Mapping property is typically used when a uid was not used as part of the user domain login name. Set the Optional User Mapping property to enabled if there is a need to convert simple user login names to domain names for user authentication. ■ State – When enabled, alternative attributes are configurable for user credential authentication. ■ Attribute Information – Enter the attribute login information using the accepted input format (&(objectclass=person)(uid=<USERNAME>)). The Attribute Information enables the LDAP/SSL query to search user domain names based on the attribute login information provided.

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/ldapssl/`
- Web: **ILOM Administration > User Management > LDAP/SSL > Settings**
- User Role: **User Management (u)** (required for all property modifications)
- Prerequisite: **LDAP/SSL server must be configured with users or user groups prior to configuring Oracle ILOM.**

Property	Default Value	Description
		■ Searchbase – Set the Searchbase property to the Distinguished Name of the search base object or to a branch in the LDAP tree where Oracle ILOM should look for LDAP user accounts. Input format: <code>OU={organization},DC={company},DC={com}</code> ■ Bind DN – Set the Bind DN property to the Distinguished Name (DN) of a read-only proxy user on the LDAP server. Oracle ILOM must have read-only access to your LDAP server to search and authenticate users. Input format: <code>OU={organization},DC={company},DC={com}</code> ■ Bind Password – Set the Bind Password property to a password for the read-only proxy user. CLI Optional User Mapping Syntax: <pre>set /SP CMM/clients/ldapssl/optionalUsermapping/ attributeInfo=<string> searchbase=<string> binddn=cn=proxyuser, ou=organization_name, dc=company, dc=com bindpw=password</pre>
Log Detail (logdetail=)	None	<i>None High Medium Low Trace</i> To specify the type of diagnostic information recorded in the Oracle ILOM event log for LDAP/SSL events, set the Log Detail property to one of the five property values accepted (none, high, medium, low or trace). CLI Log Detail Syntax: <pre>set /SP CMM/clients/ldapssl/ logdetail=none high medium low trace</pre>
Save		Web interface – To apply changes made to properties within the LDAP/SSL Settings page, you must click Save.

TABLE 26 Uploading or Removing an LDAP/SSL Certificate File**User Interface Configurable Target:**

- CLI: `/SP|CMM/clients/ldapssl/cert`
- Web: **ILOM Administration > User Management > LDAP/SSL > Certificate Information**
- User Role: **User Management (u)** (required for all property modifications)

Property	Default Value	Description
Certificate File Status (certstatus=)	Read-only	<i>Certificate Present Certificate Not Present</i> The Certificate File Status property indicates whether an LDAP/SSL certificate has been uploaded to Oracle ILOM. CLI Certificate Status Syntax: <pre>show /SP CMM/clients/ldapssl/cert</pre>
File Transfer Method	Browser (web interface only)	<i>Browser TFTP FTP SCP Paste</i>

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/ldapssl/cert`
- Web: ILOM Administration > User Management > LDAP/SSL > Certificate Information
- User Role: User Management (u) (required for all property modifications)

Property	Default Value	Description
		For a detailed description of each file transfer method, see Table 14, “ File Transfer Methods ,” on page 50.
Load Certificate (load_uri=)		Web interface – Click the Load Certificate button to upload the LDAP/SSL certificate file that is designated in the File Transfer Method property. CLI Load Certificate Syntax: load_uri=file_transfer_method://host_address/file_path/filename
Remove Certificate (clear_action=true)		Web interface – Click the Remove Certificate button to remove the LDAP/SSL certificate file presently stored in Oracle ILOM. When prompted, click Yes to continue the action or No to cancel the action. CLI Remove Certificate Syntax: set /SP CMM/clients/ldapssl/cert clear_action=true -or- reset /SP CMM/clients/ldapssl/cert When prompted, type y to continue the action or n to cancel the action.

TABLE 27 Optionally Configuring LDAP/SSL Groups**User Interface Configurable Target:**

- CLI: `/SP|CMM/clients/ldapssl`
- Web: ILOM Administration > User Management > LDAP/SSL > (Name) Groups
- User Role: User Management (u) (required for all property modifications)
- Prerequisite: Prior to setting up LDAP/SSL Groups in Oracle ILOM, the LDAP/SSL Groups must be present on the LDAP/SSL server and assigned members.

Property	Description
Admin Groups (/admingroups/1 2 3 4 5)	A system administrator can optionally configure Admin Group properties instead of the Role properties in Oracle ILOM to provide user authorization. Oracle ILOM supports the configuration of up to five Admin Groups. When Admin Group properties are enabled in Oracle ILOM, a user's group membership is checked for any matching groups defined in the admin table. If a match occurs, the user is granted Administrator-level access. Note – Oracle ILOM grants a group member one or more authorization levels based on the matching groups (operator, administrator, or custom) found in each configured group table. CLI Admin Group Syntax: set /SP CMM/clients/ldapssl/admingroups/n name=string

User Interface Configurable Target:

- CLI: `/SP/CMM/clients/ldapssl`
- Web: ILOM Administration > User Management > LDAP/SSL > (Name) Groups
- User Role: User Management (u) (required for all property modifications)
- Prerequisite: Prior to setting up LDAP/SSL Groups in Oracle ILOM, the LDAP/SSL Groups must be present on the LDAP/SSL server and assigned members.

Property	Description
	Example Syntax: <pre>set /SP/clients/ldapssl/admingroups/1/ name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com</pre> Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com'
Operator Groups	A system administrator can optionally configure Operator Group properties instead of the Role properties in Oracle ILOM to provide user authorization. (/operatorgroups/1 2 3 4 5) Oracle ILOM supports the configuration of up to five Operator Groups. When Operator Group properties are enabled in Oracle ILOM, a user's group membership is checked for any matching groups defined in the operator table. If a match occurs, the user is granted Operator-level access. Note – Oracle ILOM grants a group member one or more authorization levels based on the matching groups (operator, administrator, or custom) found in each configured group table. CLI Operator Group Syntax: <pre>set /SP/CMM/clients/ldapssl/operatorgroups/n name=string</pre> Example Syntax: <pre>set /SP/clients/ldapssl/operatorgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com</pre> Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com'
Host Groups	LDAP/SSL Host Groups properties are specific to Oracle's multi-domain SPARC server systems. For multi-domain SP server systems, Oracle ILOM enables system administrators to configure up to 10 host groups for LDAP/SSL user authentication. CLI Configuration Syntax for Host Groups: <pre>set /SP/clients/ldapssl/hostgroups/n/ name=string hosts=string roles=string</pre> Where: ■ name= is a read and write property that represents the Active Directory group name for the specified host group. ■ hosts= is a read and write property that lists the PDomain for which this host group assigns roles. ■ roles= is a read/write property that specifies the domain-specific privilege levels for the host group. This property supports any of the individual host role ID combinations of a, c, and r (for example, acr) where a= admin, c=console, and r=reset. For further details about configuring Host Group properties for multi-domain server SP systems, see the administration guide provided with the Oracle server.

User Interface Configurable Target:

- **CLI:** `/SP|CMM/clients/ldapssl`
- **Web:** ILOM Administration > User Management > LDAP/SSL > (Name) Groups
- **User Role:** User Management (u) (required for all property modifications)
- **Prerequisite:** Prior to setting up LDAP/SSL Groups in Oracle ILOM, the LDAP/SSL Groups must be present on the LDAP/SSL server and assigned members.

Property	Description
Custom Groups (/customgroups/1 2 3 4 5)	A system administrator can optionally configure up to five Custom Groups properties in Oracle ILOM to provide user authorization. Oracle ILOM uses the Custom Group properties to determine the appropriate user roles to assign when authenticating users who are members of a Custom Group When enabling the use of Custom Groups in Oracle ILOM, both the Roles property and the Custom Groups property must be configured. For further information about the configuration properties for Roles, see the Roles property in Table 25, “Enabling LDAP/SSL Authentication ,” on page 70. Note – Oracle ILOM grants a group member one or more authorization levels based on the matching groups (operator, administrator, or custom) found in each configured group table. CLI Custom Groups Syntax: <pre>set /SP CMM/clients/ldapssl/customgroups/n name=string roles=administrator operator a u c r o s</pre> Example Syntax: <pre>set /SP/clients/ldapssl/customgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com roles=au</pre> Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com' roles' to 'au' Related Information: ■ “Assignable Oracle ILOM User Roles” on page 43
Save	Web interface – To apply changes made to properties in the Admin, Operator, or Custom Group dialogs, you must click Save.

TABLE 28 Configuring LDAP/SSL User Domains**User Interface Configurable Target:**

- **CLI:** `/SP|CMM/clients/ldapssl/userdomains/n`
- **Web:** ILOM Administration > User Management > LDAP/SSL > User Domains
- **User Role:** User Management (u) (required for all property modifications)
- **Prerequisite:** Prior to setting up User Domains in Oracle ILOM, the User Domains must be present on the LDAP/SSL server and assigned members.

Property	Description
User Domains (/1 2 3 4 5)	A system administrator can optionally configure up to five User Domains. When one or more User Domains are defined, Oracle ILOM uses these properties in sequence until it is able to authenticate the LDAP/SSL user. Use the following possible values to populate the configuration properties for each User Domain in Oracle ILOM.

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/ldapssl/userdomains/n`
- Web: ILOM Administration > User Management > LDAP/SSL > User Domains
- User Role: User Management (u) (required for all property modifications)
- Prerequisite: Prior to setting up User Domains in Oracle ILOM, the User Domains must be present on the LDAP/SSL server and assigned members.

Property	Description
	■ UID format: uid=<USERNAME>,ou=people,dc=company,dc=com ■ DN format: CN=<USERNAME>,CN=Users,DC=domain,DC=company,DC=com Note - You can use <USERNAME> as a literal. When <USERNAME> is used as a literal Oracle ILOM replaces the <USERNAME> during user authentication with the current login name entered. You can optionally specify a specific searchbase by appending the <BASE:string> property after the user domain configuration. For syntax details, see Example 3 below. CLI User Domains Syntax: set <code>/SP CMM/clients/ldapssl/userdomains/n domain=string</code> Example 1: domain=CN=<USERNAME> set <code>/SP/clients/ldapssl/userdomains/1 domain=CN=<USERNAME>,OU=Groups,DC=sales,DC-oracle,DC=com</code> Set 'domain' to 'CN=<USERNAME>,OU=Groups,DC=sales,DC=oracle,DC=com' Example 2: domain=CN=spSuperAdmin set <code>/SP/clients/ldapssl/userdomains/1 domain=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com</code> Set 'domain' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com' Example 3: Searchbase syntax using <BASE:string> set <code>/SP/clients/ldapssl/userdomains/1 domain=uid=<USERNAME>,ou=people,dc=oracle,dc=com<BASE:ou=doc,dc=oracle,dc=com></code>
Save	Web interface – To apply changes made to properties in the LDAP/SSL User Domain dialog, you must click Save.

TABLE 29 Optionally Configuring LDAP/SSL Alternate Servers**User Interface Configurable Target:**

- CLI: `/SP|CMM/clients/ldapssl/alternateservers/n`
- Web: ILOM Administration > User Management > LDAP/SSL > Alternate Servers
- User Role: User Management (u) (required for all property modifications)

Property	Description
Alternate Servers	Oracle ILOM enables you to configure up to five LDAP/SSL alternate servers.

User Interface Configurable Target:

- **CLI:** `/SP|CMM/clients/ldapssl/alternateservers/n`
- **Web:** ILOM Administration > User Management > LDAP/SSL > Alternate Servers
- **User Role:** User Management (u) (required for all property modifications)

Property	Description
(/1 2 3 4 5)	Alternate servers provide authentication redundancy, as well as a choice of different LDAP/SSL servers to use when you need to isolate domains. Each LDAP/SSL alternate server uses the same user authorization rules and requirements as the primary LDAP/SSL server. For example, Oracle ILOM will use the configured user roles in the Roles property to authenticate users. However, if the Roles property is not configured, Oracle ILOM will query the authentication server for the appropriate authorization roles. Each alternate server has its own properties for network address, port, certificate status, and commands for uploading and removing a certificate. If an LDAP/SSL certificate is not supplied, but is required, Oracle ILOM will use the top-level primary LDAP/SSL server certificate. CLI Alternate Servers Address and Port Syntax: <pre>set /SP CMM/clients/ldapssl/alternateservers/n address=string port=string</pre> CLI Alternate Server s Certificate Syntax: <pre>show /SP CMM/clients/ldapssl/alternateservers/n/cert</pre> <pre>load_uri=file_transfer_method://host_address/file_path/filename</pre> <pre>set /SP CMM/clients/ldapssl/alternateservers/n/cert clear_action=true</pre>
Save	Web interface – To apply changes made to properties in the LDAP/SSL Alternate Servers dialog, you must click Save.

TABLE 30 Guidelines for Troubleshooting LDAP/SSL Authentication

Refer to the following guidelines when troubleshooting LDAP/SSL authentication and authorization attempts in Oracle ILOM.

- To test LDAP/SSL authentication and set the Oracle ILOM event log to trace LDAP/SSL events, follow these steps:
 - 1: Set the LDAP/SSL Log Details property to trace.
 - 2: Attempt an authentication to Oracle ILOM to generate events.
 - 3: Review the Oracle ILOM event log file.
 - Ensure that the user groups and user domains configured on the LDAP/SSL server match the user groups and user domains configured in Oracle ILOM.
 - The Oracle ILOM LDAP/SSL Client does not manage clock settings. The clock settings in Oracle ILOM are configurable manually or through an NTP server.
- Note.** When the clock setting in Oracle ILOM is configured using an NTP server, Oracle ILOM performs an ntpdate using the NTP server(s) before starting the NTP daemon.

Related Information:

- [Table 25, “Enabling LDAP/SSL Authentication ,” on page 70](#)
- [“Managing Oracle ILOM Log Entries” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

-
- [“Setting ILOM Clock Properties” on page 142](#)
-

Configuring LDAP

System administrators can configure Oracle ILOM to use the Lightweight Directory Access Protocol (LDAP) service to authenticate users. This service is based on a client-server query model that uses a read-only proxy user account to query the LDAP server for user authentication.

The property for the LDAP service state, in Oracle ILOM, is disabled by default. To enable the LDAP service state and configure properties for using the LDAP directory service for user authentication, see these tables:

- [Table 31, “Requirements for Enabling Oracle ILOM as an LDAP Client,” on page 79](#)
Requirements for Enabling Oracle ILOM as an LDAP Client
- [Table 32, “Enabling Oracle ILOM to Use LDAP Authentication,” on page 80](#) Enabling Oracle ILOM to Use LDAP Authentication

TABLE 31 Requirements for Enabling Oracle ILOM as an LDAP Client

Prior to configuring Oracle ILOM as an LDAP client, the LDAP server must be properly configured. Refer to the following guidelines, and Related Information section, when configuring the LDAP server to recognize Oracle ILOM as an LDAP client.

- Ensure that the LDAP server is set to use the default password {crypt} format. The passwords for all LDAP users authenticating to Oracle ILOM must be stored in one of the following two {crypt} formats:
 userPassword: {CRYPT}ajCa2He4PJhNo
 userPassword: {CRYPT}\$1\$pzKng1\$du1Bf0NWBjh9t3FbUgf46
- Refer to the Internet Engineering Task Force Schema (RFC 2307) for adding object classes for posixAccount and shadowAccount and then populate the required property values for:
 - *uidnumber*
 - *gidnumber*
 - *uid* (Oracle ILOM user name),
- Enable the LDAP server to accept anonymous binds, or create a proxy user on the LDAP server to have read-only access for all user accounts authenticating to Oracle ILOM.

Related Information:

- Internet Engineering Task Force Schema (RFC2307) (<http://www.ietf.org/rfc/rfc2307.txt>)
-

TABLE 32 Enabling Oracle ILOM to Use LDAP Authentication

User Interface Configurable Target:		
■ CLI: <code>/SP CMM/clients/ldap</code> ■ Web: ILOM Administration > User Management > LDAP Settings ■ User Role: User Management (u) (required for all property modifications)		
Property	Default Value	Description
State (state=)	Disabled	<i>Disabled Enabled</i> To enable Oracle ILOM to authenticate users using the LDAP directory service, set the State property to enabled. When the State property is enabled, Oracle ILOM queries the LDAP server to authenticate LDAP users. CLI State Syntax: set <code>/SP CMM/clients/ldap/ state=disabled enabled</code>
Roles (defaultrole=)	Operator	<i>Administrator Operator Advanced</i> To define which features in Oracle ILOM are accessible to LDAP authenticated users, set the default Roles property to one of three Oracle ILOM user roles: Administrator (a u c r o), Operator (c r o), or Advanced (a u c r o s) Authorization levels for using features within Oracle ILOM are dictated by the user privileges granted by the configured Oracle ILOM user role. For a description of privileges assigned, see the user role and user profile topics listed in the Related Information section below. CLI Roles Syntax: set <code>/SP CMM/clients/ldap/ defaultrole=administrator operator a u c r o s</code> Related Information: ■ Table 10, “Privileges Granted by a User Profile,” on page 44 ■ Table 11, “Privileges Granted by Individual User Roles,” on page 45
Address (address=)	0.0.0.0	<i>IP address DNS host name (LDAP Server)</i> To configure the LDAP server network address, populate the Address property with the LDAP server IP address or DNS host name. If a DNS host name is used, then the DNS configuration properties in Oracle ILOM must be properly configured and operational. CLI Address Syntax: set <code>/SP CMM/clients/ldap/ address=ldap_server ip_address ldap_server_dns_host_name</code> Related Information: ■ Table 48, “DNS Configuration Properties ,” on page 134
Port (port=)	389	<i>389 User-specified TCP port</i> TCP port 389 is used by Oracle ILOM to communicate with the OpenLDAP server.

User Interface Configurable Target:

- CLI: */SP|CMM/clients/ldap*
- Web: **ILOM Administration > User Management > LDAP Settings**
- User Role: **User Management (u)** (required for all property modifications)

Property	Default Value	Description
		If necessary, configure Oracle ILOM to use another port by modifying the default Port number: 389 CLI Port Syntax: set /SP CMM/clients/ldap/ port=number
Searchbase (searchbase=)		<i>ou=organization_unit dn=domain_name dc=domain </i> The Searchbase is the location in the LDAP tree where Oracle ILOM searches to validate user credentials. Using the accepted input format, populate the Searchbase property with a Distinguished Name for the search base object, or with the LDAP tree branch for where Oracle ILOM should search for the LDAP user accounts. For example, to search the IT container in the MyCompany.com domain, you would specify a search base of: <i>ou=IT, dc=mycompany, dc=.com</i> CLI Searchbase Syntax: set /SP CMM/clients/ldap/ searchbase= ou=organization_name, dn=domain_name, dc=domain
Bind DN (binddn=)		<i>ou=organization_unit dn=domain_name dc=domain cn=common_name</i> To provide Oracle ILOM with read-only access to the LDAP server, populate the Bind DN property with a Distinguished Name (DN) for a read-only proxy user. Note. Oracle ILOM must have read-only access to the LDAP server in order to search and authenticate LDAP users. CLI Bind DN Syntax: set /SP CMM/clients/ldap/ binddn=cn=proxyuser, ou=organization_name, dc=domain
Bind Password (bindpw=)		To provide Oracle ILOM with a password for the read-only proxy user, populate the Bind Password property with a password. CLI Bind Password Syntax: set /SP CMM/clients/ldap/ bindpw=password
Save		Web interface – To apply changes made to properties within the LDAP Settings page, you must click Save.

Configuring RADIUS

System administrators can configure Oracle ILOM to use a Remote Authentication Dial-In User Service (RADIUS) to authenticate users. This service is based on a client-server query model that uses a shared secret password to authenticate users. The Oracle ILOM RADIUS client and RADIUS server must know the shared secret password since this password is never transmitted over the network.

The property for the RADIUS service state, in Oracle ILOM, is disabled by default. To enable the RADIUS service state and configure Oracle ILOM properties as a RADIUS client, see the following table.

TABLE 33 Enabling Oracle ILOM to Use RADIUS Client Server Authentication

User Interface Configurable Target:		
■ CLI: <code>/SP CMM/clients/radius</code> ■ Web: ILOM Administration > User Management > RADIUS Settings ■ User Role: User Management (u) (required for all property modifications) ■ Requirement: The RADIUS server must be preconfigured with users and the shared secret password.		
Property	Default Value	Description
State	Disabled	<i>Disabled Enabled</i>
(state=)		To configure Oracle ILOM as a RADIUS client, set the State Property to Enabled. When the State property is enabled, Oracle ILOM sends user login data to the RADIUS server for user authentication and authorization. CLI RADIUS State Syntax: set /SP CMM/clients/radius/ state=disabled enabled
Roles	Operator	<i>Administrator Operator Advanced</i>
(defaultrole=)		To define which features in Oracle ILOM are accessible to RADIUS authenticated users, set the default Roles property to one of the three Oracle ILOM user roles: Administrator (a u c r o), Operator (c r o), Advanced (a u c r o s). Authorization levels for using features within Oracle ILOM are dictated by the privileges granted by the configured Oracle ILOM user role. For a description of privileges assigned, see the user role and user profile tables listed in the Related Information section below. CLI Roles Syntax: set /SP CMM/clients/radius/ defaultrole=administrator operator a u c r o s Related Information: ■ Table 10, “Privileges Granted by a User Profile,” on page 44 ■ Table 11, “Privileges Granted by Individual User Roles,” on page 45

User Interface Configurable Target:

- CLI: `/SP|CMM/clients/radius`
- Web: ILOM Administration > User Management > RADIUS Settings
- User Role: User Management (u) (required for all property modifications)
- Requirement: The RADIUS server must be preconfigured with users and the shared secret password.

Property	Default Value	Description
Address (address=)	0.0.0.0	<i>IP address DNS host name (LDAP Server)</i> To configure a network address for RADIUS server, populate the Address property with the RADIUS server IP address or DNS host name. If a DNS host name is specified, then the DNS configuration properties in Oracle ILOM must be properly configured and operational. CLI Address Syntax: <pre>set /SP CMM/clients/radius/ address=radius_server ip_address ldap_server_dns_host_name</pre> Related Information: ■ Table 48, “DNS Configuration Properties ,” on page 134
Port (port=)	1812	<i>1812 User-specified TCP port</i> TCP port 1812 is used by Oracle ILOM to communicate with the RADIUS server. If necessary, configure Oracle ILOM to use another port by modifying the default Port number: 1812 CLI Port Syntax: <pre>set /SP CMM/clients/radius/ port=number</pre>
Shared Secret (secret=)		Populate the Shared Secret property with the known RADIUS client server shared password. The RADIUS client server model uses the shared password to recognize each other, and to protect sensitive user credential data. CLI Shared Secret Syntax: <pre>set /SP CMM/clients/radius/ secret=password</pre>
Alternate RADIUS Servers	N/A	In cases where the primary RADIUS server is unavailable, you can optionally configure Oracle ILOM to use an alternate RADIUS server for user authentication. You can specify up to 5 alternate RADIUS server configurations. Note - The properties for Alternate RADIUS Servers is available for configuration as of Oracle ILOM 3.2.6. For web configuration instructions, click the More details ... link at the top of the User Management RADIUS page. CLI Alternate RADIUS Servers: <pre>set /SP CMM/clients/radius/alternateservers/1 2 3 4 5/ address=radius_server ip_address ldap_server_dns_host_name port=number secret=password</pre>

User Interface Configurable Target:

- **CLI:** `/SP|CMM/clients/radius`
- **Web:** ILOM Administration > User Management > RADIUS Settings
- **User Role:** User Management (u) (required for all property modifications)
- **Requirement:** The RADIUS server must be preconfigured with users and the shared secret password.

Property	Default Value	Description
		Note - In the case of a failover, Oracle ILOM will query the alternate server ID configurations in the order they are listed. For example, ID 1, ID 2, and so on.
Save		Web interface. To apply changes made to properties within the RADIUS Settings page, you must click Save.

Modifying Default Settings for Network Deployment and Administration

Description	Links
Refer to this section to better understand Oracle ILOM's deployment options and default settings for management access and network connectivity.	■ “Network Deployment Principles and Considerations” on page 85
Refer to this section for management access requirements and configuration properties.	■ “Modifying Default Management Access Configuration Properties” on page 100
Refer to this section for connectivity requirements and configuration properties.	■ “Modifying Default Connectivity Configuration Properties” on page 118
Refer to these sections for instructions on how to set up system identification labels and set the date and time properties in Oracle ILOM.	■ “Assigning System Identification Information” on page 140 ■ “Setting ILOM Clock Properties ” on page 142
Refer to this section for guidelines for resolving management access and network connectivity issues.	■ “Suggested Resolutions for Network Connectivity Issues” on page 143

Related Information

- *Oracle ILOM Security Guide (3.2.x)*, deployment considerations
- [“Logging In to Oracle ILOM” in *Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*](#)

Network Deployment Principles and Considerations

When setting up Oracle ILOM on a network, it is important to understand the initial network settings shipped with Oracle ILOM, as well as other configurable options network administrators can choose to implement.

For information about network deployment options for Oracle ILOM, and general information to consider when managing Oracle ILOM in a network environment, see these topics:

- [“Network Management Service Deployment Options” on page 86](#)
- [“Network Connectivity Deployment Options” on page 88](#)

- [“Operating Oracle ILOM in FIPS Compliance Mode” on page 89](#)
- [“Management of SSH Server State and Weak Ciphers” on page 93](#)
- [“Use of Web Server Certificates and SSH Server-Side Keys” on page 93](#)
- [“Default Timeout for CLI and Web Sessions” on page 93](#)
- [“Management of Banner Messages at Log-In” on page 94](#)
- [“Input Format for IPv4 and IPv6 Addresses” on page 98](#)
- [“Serial Management Port Owner” on page 98](#)
- [“Default Network Ports Used by Oracle ILOM” on page 99](#)
- [“Legacy Oracle Servers Not Supporting IPv6” on page 100](#)

Network Management Service Deployment Options

Oracle ILOM supports the configuration of several network management services. Some of these services are enabled by default, while others require configuration. To better understand which management services arrive enabled, and which management services are actually required for your network environment, see the following table.

Note - You should only enable the management services that are required for your network management environment.

TABLE 34 Management Access Deployment Options and Default Settings

Management Access	Management Service	Defaults	Description
Web browser client	■ Web Server	■ HTTPS over port 443 enabled ■ TLS v1.2 enabled ■ TLS v1.1 disabled by default. ■ SSL certificate & self-signing keys ■ Client timeout session, 15 minutes ■ FIPS compliance mode disabled	The Web Server management service in Oracle ILOM, by default, enables a secure communication channel between a web browser client and the Oracle ILOM SP or CMM. Network administrators can accept the default web server properties provided in Oracle ILOM or choose to modify them as needed. Related Information: ■ “Operating Oracle ILOM in FIPS Compliance Mode” on page 89 ■ “Use of Web Server Certificates and SSH Server-Side Keys” on page 93 ■ Table 38, “Web Server Configuration Properties,” on page 101

Management Access	Management Service	Defaults	Description
Command-line SSH client	Secure Shell (SSH) Server	- Port 22 enabled - Generated SSH keys - Client timeout session, unlimited - FIPS compliance mode disabled	The SSH Server service in Oracle ILOM uses server-side keys to encrypt the management channel between an SSH command-line client and an Oracle ILOM SP or CMM. Oracle ILOM automatically generates the server-side SSH keys on the first boot of a factory default system. Related Information: - Table 41, “SSH Server Configuration Properties,” on page 110 “Operating Oracle ILOM in FIPS Compliance Mode” on page 89 “Use of Web Server Certificates and SSH Server-Side Keys” on page 93
SNMP application client	Simple Network Management Protocol (SNMP)	- SNMPv3 over port 161, enabled - SNMP sets disabled - User account configuration required - FIPS compliance mode disabled	The SNMP management service in Oracle ILOM offers a secure protocol management solution for monitoring and managing Oracle servers. All SNMP monitoring and management functionality is accessible from an SNMP application, such as Net-SNMP. Prior to using the SNMP management service in Oracle ILOM, one or more Oracle ILOM user accounts must be created. Additionally, prior to using SNMP sets, the SNMP sets property must be enabled. Oracle ILOM is shipped with SNMPv3 enabled, although administrators can optionally choose to enable the properties for SNMPv1 or SNMPv2c. Related Information: - Table 40, “SNMP Configuration Properties,” on page 107 “Operating Oracle ILOM in FIPS Compliance Mode” on page 89 “Configuring SNMP Settings in Oracle ILOM” in <i>Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x</i> “Alert Notification Configuration Properties” on page 262
IPMItoolclient	IPMI	- IPMPv2 over port 623, enabled - IPMI Service state enabled - IPMI 1.5 disabled by default (as of 3.2.4)	The IPMI management service in Oracle ILOM offers a secure protocol solution for monitoring and managing Oracle servers. IPMI monitoring and management functionality is accessible from the Oracle ILOM CLI using the IPMItool utility. IPMI configurable properties in Oracle ILOM include the IPMI management service state and the required user roles (Administrator or Operator) for performing IPMI management functions from the Oracle ILOM CLI.

Management Access	Management Service	Defaults	Description
			Note - As of firmware 3.2.4, a configurable property for enabling and disabling IPMI 1.5 is provided. This property is removed from the user interfaces when FIPS mode is enabled. Related Information: ■ Table 42, “IPMI Service Configuration Properties,” on page 112 ■ “Operating Oracle ILOM in FIPS Compliance Mode” on page 89 ■ “Assignable Oracle ILOM User Roles” on page 43 ■ “Server Management Using IPMI” in <i>Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x</i> ■ “Alert Notification Configuration Properties” on page 262

Network Connectivity Deployment Options

The connectivity options in Oracle ILOM arrive preconfigured so Oracle ILOM can learn the physical server SP or CMM network address. To better understand which connectivity properties are shipped enabled, and which connectivity properties are required for your network environment, see the following table.

TABLE 35 Connectivity Deployment Options and Default Settings

Connectivity Options	Defaults	Description
Network	■ IPv 4, DHCP enabled ■ IP 6, Stateless, enabled ■ Management Port: MGMT	Oracle ILOM, by default, arrives configured to operate in a dual-stack IPv4 and IPv6 network environment. Upon setting a physical network management connection to the server or CMM, Oracle ILOM will attempt to learn the physical address for the SP or CMM from the IP mapping and routing devices configured on the network. Network administrators can accept the default dual-stack IP network properties in Oracle ILOM, or choose to disable them and configure the required IP network properties. Related Information: ■ Table 46, “Network Connectivity Standard Configuration Properties ,” on page 119 ■ “Sideband Network Management Connection” on page 20 ■ “Dedicated Network Management Connection (Default)” on page 18
DNS	■ Auto DNS via DHCP, enabled ■ DNS timeout 5 seconds ■ DNS retries 1	The Auto DNS property in Oracle ILOM uses DHCP to automatically assign the DNS named server and search path.

Connectivity Options	Defaults	Description
		Network administrators can accept the default Auto DNS properties in Oracle ILOM or choose to disable them and configure the required DNS name server and search path. Related Information: ■ Table 48, “DNS Configuration Properties ,” on page 134 ■ “Example Setup of Dynamic DNS” on page 137
Serial Ports	■ Owner= SP ■ Baud Rate: = 9600 ■ Flow Control = none	The console output functionality for the physical serial management port on the server is controlled by the server SP. Network administrators can accept the server SP as the default serial port owner, or switch the port ownership to the host server operating system. On most servers, the default baud rate is set, by default, to 9600. Related Information: ■ Table 49, “Serial Port Configuration Properties ,” on page 136 ■ “Serial Management Port Owner” on page 98 ■ “Dedicated Network Management Connection (Default)” on page 18

Operating Oracle ILOM in FIPS Compliance Mode

As of Oracle ILOM firmware release 3.2.4, the Oracle ILOM CLI and web interface provide a configurable mode for Federal Information Processing Standards (FIPS) Level 1 compliance. When this mode is enabled, Oracle ILOM provides cryptographic algorithms in compliance with the FIPS 140-2 security standards for protecting system sensitive or valuable data.

The FIPS mode State and Status properties in Oracle ILOM are disabled by default. For further details about these properties, as well as to understand the effect the FIPS mode functionality can have on other Oracle ILOM features, see the following:

- [“Modify FIPS Mode ” on page 89](#)
- [“FIPS Compliance Mode Effect on ILOM Configuration Properties” on page 91](#)
- [“Unsupported Features When FIPS Mode Is Enabled” on page 92](#)

▼ Modify FIPS Mode

Before You Begin

- Prior to modifying the FIPS mode in Oracle ILOM, you should review [“FIPS Compliance Mode Effect on ILOM Configuration Properties” on page 91](#) and [“Unsupported Features When FIPS Mode Is Enabled” on page 92](#).

- The Admin (a) role in Oracle ILOM is required to configure the FIPS State property in the CLI and web interface.
- After modifying the FIPS State property, an Oracle ILOM reboot is required to change the FIPS operational mode on the system and to update the FIPS Status property in the CLI and web interface.

The FIPS mode in Oracle ILOM is represented by the State and Status properties. The State property reflects the FIPS configured mode in Oracle ILOM, and the Status property reflects the FIPS operational mode of the system. By default, the FIPS State and Status properties in Oracle ILOM are disabled. To modify the FIPS State and Status properties in Oracle ILOM, follow these steps:

1. Navigate to the Oracle ILOM FIPS web page or the FIPS CLI target:

- **For web, click ILOM Administration > Management Access > FIPS.**
- **For CLI, type `cd /SP/services/fips`**
(or from a CMM, type: `cd /Servers/Blades/BLn/SP/services/fips`)

2. Configure the FIPS State property as described in [Table 44, “Federal Information Processing Standards \(FIPS 140-2\) Configuration Properties,” on page 116](#).

The FIPS operational change on the system will not take affect until the next Oracle ILOM boot. To determine the FIPS operational mode that is currently running on your system, view the Status property on the Management Access > FIPS web page, or view it under the FIPS CLI target (**show /SP/services/fips**). For further details, see the Status descriptions in [Table 44, “Federal Information Processing Standards \(FIPS 140-2\) Configuration Properties,” on page 116](#).

3. Reset the SP from the Oracle ILOM CLI or web interface, for instance:

- **For web, click ILOM Administration > Maintenance > Reset.**
If necessary, click the More Details link on the Reset page for instructions on how to reset the SP.
- **For CLI, type `reset /SP`**
(or from CMM, type `reset /Servers/Blades/BLn/SP`).

Upon resetting Oracle ILOM, the following events will occur:

- The last configured state for FIPS mode is applied on the system.

- A power-on self-test automatically is performed to ensure that Oracle ILOM and other system components are functional. When FIPS mode is enabled, cryptographic algorithm tests are run on all system cryptographic functions to ensure FIPS 140-2 compliance.
- Upon a successful power-on self-test, the ILOM configuration properties are automatically reset to their default values.
- The FIPS Status property is automatically updated on the FIPS web page and under the FIPS CLI target (**show /SP/services/fips**).
- When FIPS mode is enabled and running on the system, a FIPS shield icon appears in the masthead area of the Oracle ILOM web browser window. Otherwise, if FIPS mode is disabled on the system, a FIPS shield icon will not appear in the masthead area of the Oracle ILOM web browser window.

FIPS Compliance Mode Effect on ILOM Configuration Properties

Any change to the FIPS State property will automatically cause all user-defined configuration settings in Oracle ILOM to be reset to their default values upon the next ILOM boot. To avoid the loss of user-defined configuration settings, you should review the following guidelines prior to: 1) deploying a new server with FIPS mode, or 2) updating the Oracle ILOM firmware and modifying the FIPS mode on a server in an existing environment.

TABLE 36 Guidelines for Deploying a Server or Updating a Server with FIPS Mode

Guideline	Description
New Server Deployment with FIPS Mode	To avoid the loss of user-defined configuration settings in Oracle ILOM when deploying a new server with FIPS mode, you should: 1. Decide if FIPS mode is needed. 2. If FIPS mode is required, enable FIPS mode prior to configuring the Oracle ILOM configuration settings.
Update the Oracle ILOM Firmware and Modify the FIPS Mode State on Server in Existing Environment	To avoid the loss of user-defined configuration settings when updating the Oracle ILOM firmware and modifying the FIPS State property on an existing server, you should: 1. Back up the existing Oracle ILOM configuration settings: ■ In the web, navigate to ILOM Administration > Configuration Management > Backup/Restore page. ■ For additional backup instructions, click the More Details link on the Backup/Restore page in the web interface; or, see “Back Up the Oracle ILOM Configuration Settings” on page 308. 2. Perform an Oracle ILOM firmware update: ■ In the web, navigate to ILOM Administration > Maintenance > Firmware Update page. ■ To simplify reconnecting to Oracle ILOM when the firmware update is complete, you should enable the firmware update option for "Preserve the ILOM Configuration" (or, "Preserve the SP Configuration").

Guideline	Description
	■ For additional firmware update instructions, click the More Details link on the Firmware Update page in the web interface; or, see “Updating Oracle ILOM Firmware” on page 293. 3. Modify the FIPS mode (which will reset the configuration in Oracle ILOM and require a reboot): ■ In the web, navigate to ILOM Administration > Management Access > FIPS page. For further instructions, see “Modify FIPS Mode ” on page 89. 4. Restore the backed-up Oracle ILOM configuration: ■ In the web, navigate to ILOM Administration > Configuration Management > Backup/Restore page. ■ For additional restore instructions, click the More Details link on the Backup/Restore page in the web interface; or, see “Restore the Oracle ILOM Backup XML File” on page 313. Note - If you perform Step 2 prior to Step 1, you will need to edit the backed-up XML configuration file and remove the FIPS setting prior to restoring the configuration file in Step 4. Otherwise, you will have an inconsistent configuration between the backed-up Oracle ILOM XML configuration file and the FIPS mode state running on the server, which is not allowed.

Unsupported Features When FIPS Mode Is Enabled

The features described in the following table are unsupported when the FIPS compliance mode in Oracle ILOM is enabled and running on the system.

Unsupported Feature	Description
IPMI 1.5	When FIPS mode is enabled and running on the system, the IPMI 1.5 configuration property is removed from the Oracle ILOM CLI and web interface. The IPMI 2.0 service is automatically enabled in Oracle ILOM. IPMI 2.0 supports both FIPS compliant and non-compliant modes.
Firmware Compatibility for Oracle ILOM System Remote Console	FIPS mode in Oracle ILOM prevents the earlier firmware versions of Oracle ILOM Remote System Console to be compatible with the later Oracle ILOM Remote System Console firmware versions. For instance, the Oracle ILOM Remote System Console Client firmware version 3.2.4 is backward compatible with the Oracle ILOM Remote System Console firmware version 3.2.3 and earlier. However, the Oracle ILOM Remote System Console Client firmware version 3.2.3 and earlier are not forward compatible with the Oracle ILOM Remote System Console firmware version 3.2.4 and later. Note - This firmware compatibility limitation does not apply to the Oracle ILOM Remote System Console Plus. The Oracle ILOM Remote System Console Plus is provided on newer service processor systems such as, SPARC T5 and later and Oracle x86 servers such as x4-4, x4-8 and later. The Oracle ILOM Remote System Console is provided on earlier service processor systems such as, SPARC T3 and T4 and Oracle x86 servers such as x4-2, x4-2L, x4-2B, and earlier systems.
Lightweight Directory Access Protocol (LDAP)	When FIPS mode is enabled and running on the system, the LDAP configuration properties in Oracle ILOM are automatically removed from the Oracle ILOM CLI and web interface.

Unsupported Feature	Description
	Note - The following remote authentication services are supported in both FIPS compliant and non-compliant modes: Active Directory and LDAP/SSL.
Remote Authentication Dial-In User Service (RADIUS)	When FIPS mode is enabled and running on the system, the RADIUS configuration properties in Oracle ILOM are automatically removed from the Oracle ILOM CLI and web interface. Note - The following remote authentication services are supported in both FIPS compliant and non-compliant modes: Active Directory and LDAP/SSL.

Management of SSH Server State and Weak Ciphers

Oracle ILOM arrives with the SSH Server State property enabled and, as of firmware 3.2.5, the SSH Weak Ciphers property disabled. Administrators can choose to use these default settings as is or modify them. For further details about configuring these properties, see [Table 41, “SSH Server Configuration Properties,” on page 110](#).

Use of Web Server Certificates and SSH Server-Side Keys

Oracle ILOM arrives preconfigured with a web server self-signed certificate and a set of generated SSH server-side keys, which enable Oracle ILOM to ensure the authenticity of a server or client.

Network administrators can optionally choose to use the out-of-box self-signed web server certificate or upload a signed web server certificate to Oracle ILOM. Additionally, the generated SSH server-side keys can be regenerated as needed.

For further details about web server certificate configuration properties, see [Table 39, “SSL Certificate and Private Key Configuration Properties for HTTPS Web Server,” on page 104](#).

For further details about SSH server-side key configuration properties, see [Table 41, “SSH Server Configuration Properties,” on page 110](#).

Default Timeout for CLI and Web Sessions

Oracle ILOM provides configurable properties that control the amount of minutes a web or command-line client can be inactive before Oracle ILOM terminates the session.

The default timeout session for authorized web users is set to 15 minutes, and the default timeout session set for authorized command-line users is 0 minutes (which means no set CLI default timeout). To prevent unauthorized use of an unattended session, you should configure a suitable timeout for all web and CLI users.

For CLI session timeout configuration properties, see [Table 43, “CLI Session Timeout and Custom Prompt Configuration Properties,” on page 114](#). For web session timeout configuration properties, see [Table 38, “Web Server Configuration Properties,” on page 101](#).

Management of Banner Messages at Log-In

The Banner Message properties in Oracle ILOM enable system administrators to display important messages to Oracle ILOM users at either pre-login or immediately after login. For instance, system administrators can optionally use banner messages to alert users of special access restrictions or to inform users of scheduled system maintenance.

For further details about banner message configuration, see the following sections:

- [“Create or Update a Banner Message” on page 94](#)
- [“Delete a Banner Message” on page 96](#)
- [“Control Message Acceptance Behavior for Login Message” on page 97](#)

Before You Begin

- The Admin (a) role is required to configure banner messages.
- The length of the banner message cannot exceed 10,000 characters.
- The Connect Message, when configured, displays the banner message at pre-login.
- The Login Message, when configured, displays the banner message immediately after login.
- System administrators can optionally choose to configure both banner messages, one banner message, or none at all.

▼ Create or Update a Banner Message

1. To specify the type of banner that you want to create or update, perform the applicable Web or CLI step:
 - **Web:** Click **Update** under either the **Connect** or **Login** message text box.
The Edit Banner Message dialog appears.
 - **CLI:** Type the following command string:

```
cd /[SP | CMM]/preferences/banner/[connect | login]
```

where:

- SP = Server SP management
- CMM = Chassis management (Chassis Monitoring Module)
- connect = Pre-login message
- login = Post-login message

2. To specify the banner message, perform the applicable Web or CLI steps.

- **Web:** In the Edit Banner Message dialog, perform one of the following actions.
 - To paste or type a message in the Data text box, select Paste from the Transfer Method box, enter the text into the Data text box, and then click Save.
 - To upload content from a file, select a protocol from the Transfer Method box, fill in the appropriate Transfer Method text boxes, and then click Save.
For a description of each file transfer protocol, see [“Supported File Transfer Methods” on page 50](#).
- **CLI:** To paste, upload, or type a message, perform one of the following:
 - To paste a message from a target location:
 - a Type the following command string
load -source console

Note - Setting the message via console only supports 1000 characters.

- b Paste the message below the command string that was typed in Step 2a.
- c Press one of the following key-combinations:
 - **Ctrl-Z — To save and process the changes.**
A Load Successful confirmation message appears.

- **Ctrl-C** —To exit and discard the changes.
- **To manually enter message content, type the following command string:**
`set message=[message content]`
- **To upload message content by using a file transfer protocol, type the following command string:**
`load -source URI [file transfer protocol]://[username:password@ipaddress_or_hostname]/[file-path]/[filename]`
where:
 - *file transfer method* = *tftp* | *ftp* | *sftp* | *scp* | *http* | *https*
For a description of each file transfer protocol, see [“Supported File Transfer Methods” on page 50](#).
 - *username* = The name of the user account for the chosen transfer method server. A username is required for scp, sftp, and ftp. A username is not required for tftp, and it is optional for http and https.
 - *password* = The user account password for the chosen transfer method server. A password is required for scp, sftp, and ftp. A password is not used for tftp, and it is optional for http and https.
 - *ipaddress_or_hostname* = Type the IP address or the host name for the chosen transfer method server.
 - *filepath* = Type the file location on the transfer method server.
 - *filename* = Type the name assigned to the file, for example: foo.xml

▼ Delete a Banner Message

- **To delete a banner message, perform the applicable Web or CLI step:**
 - **Web: Click Delete under the Connect or Login message text box.**
Oracle ILOM displays a prompt to confirm that you want to delete the banner message.
In the message prompt, click OK to delete the banner message or click Cancel to keep the banner message.
 - **CLI: Type the following command string:**
`set /[SP | CMM]/preferences/banner/[connect | login] message=""`
where:

- *SP* = Server SP management
- *CMM* = Chassis management (Chassis Monitoring Module)
- *connect* = The pre-login message.
- *login* = The post-login message.

▼ Control Message Acceptance Behavior for Login Message

- To control the message acceptance behavior for the Login message, perform the applicable Web or CLI step(s):

- **Web: Set the applicable message acceptance behavior:**

- **To prompt for acceptance:**

- a **Select the check box for Login Message Acceptance Enabled.**

When the Enabled check box is selected, the user is prompted to accept the conditions of the Login message by clicking Accept or Logout. Clicking Accept will continue the login process and clicking Logout will exit the login process.

- b **Click Save.**

- **To continue without acceptance:**

- a **Clear the check box for Login Message Acceptance Enabled.**

When the Enabled check box is cleared, the user is prompted to continue the login process by clicking OK. The Enabled check box is cleared by default.

- b **Click Save.**

- **CLI: Type the following command string to set the applicable message acceptance behavior:**

```
set /[SP | CMM]/preferences/banner/login message_acceptance= [enabled | disabled]
```

where:

- *SP* = Server SP management
- *CMM* = Chassis management (Chassis Monitoring Module)
- *enabled* = User is prompt to accept the conditions of the Login message by clicking Accept or Logout.

- *disabled* = User is prompted to continue the login process by clicking OK.

Input Format for IPv4 and IPv6 Addresses

Oracle ILOM accepts the following input format for IPv4 and IPv6 addresses.

Address	Input Format
IPv4 (32 bit)	Use a four dotted-decimal number: <i>n.n.n.n</i> Example: 192.0.2.0
IPv6 (128 bit)	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. Examples: ■ IPv6 address: [2001:db8:0:0:0:0:0:0/32] ■ IPv6 address using SSH and root account: ssh root@2001:db8:0:0:0:0:0:0/32 ■ Link-Local IPv6 address: [fe80::214:4fff:feca:5f7e/64]

Serial Management Port Owner

All Oracle servers with Oracle ILOM are shipped with the output display of the SER MGT port set to the server SP. However, on some Oracle servers, Oracle ILOM provides a property that enables network administrators to switch the ownership of the serial port between the server SP (default) and the host server operating system.

When the owner for the serial port is switched to the host server, the host operating system controls the functionality of the serial port and the server SP has no control or access to the serial port.

Prior to switching the serial port owner to the host server, network administrators should ensure that a network management connection has been established to the server SP. Otherwise, without a network management connection and with the host server property set as the serial port owner, the Oracle ILOM SP will become locally and remotely inaccessible to all users.

To modify the default property for the serial port owner in Oracle ILOM, see [Table 49, “Serial Port Configuration Properties,”](#) on page 136.

Default Network Ports Used by Oracle ILOM

To determine which network ports Oracle ILOM uses by default (out-of-box), see the following table:

TABLE 37 Oracle ILOM Default Network Ports

Port	Protocol	Application
Common Network Ports		
22	SSH over TCP	SSH - Secure Shell
25	SMTP over TCP	SMTP client communication
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol (outgoing)
80	HTTP over TCP	Web (user-configurable)
123	NTP over UDP	NTP - Network Time Protocol (outgoing)
161	SNMP over UDP	SNMP - Simple Network Management Protocol (user-configurable)
162	IPMI over UDP	IPMI - Platform Event Trap (PET) (outgoing)
163	IPMI over UDP	IPMI - LAN and LANPlus interface sessions.
163	IPMI over TCP	IPMI - TLS interface sessions (as of Oracle firmware 3.2.8).
389	LDAP over UDP/TCP	LDAP - Lightweight Directory Access Protocol (outgoing; user-configurable)
443	HTTPS over TCP	Web (user-configurable)
514	Syslog over UDP	Syslog - (outgoing)
623	IPMI over UDP	IPMI - Intelligent Platform Management Interface
546	DHCP over UDP	DHCP - Dynamic Host Configuration Protocol (client)
1812	RADIUS over UDP	RADIUS - Remote Authentication Dial-In User Service (outgoing; user-configurable)
SP Network Ports		
5120	TCP	Oracle ILOM Remote System Console: CD, or, Oracle ILOM Remote System Console Plus: Non-SSL Encryption for storage media
5121	TCP	Oracle ILOM Remote System Console: Keyboard and Mouse
5123	TCP	Oracle ILOM Remote System Console: Diskette
5555	TCP	Oracle ILOM Remote System Console: Encryption, or, Oracle ILOM Remote System Console Plus: SSL Encryption for storage, video, and user authentication.
5556	TCP	Oracle ILOM Remote System Console ILOM Remote System Console: Authentication
5122	TCP	Oracle ILOM Remote System Console
7578	TCP	Oracle ILOM Remote System Console: Video
7579	TCP	Oracle ILOM Remote System Console: Serial
CMM Network Ports		

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

Legacy Oracle Servers Not Supporting IPv6

For a list of legacy Oracle server SPs currently not supporting IPv6, see the following table.

Oracle Platform	Server Model
SPARC Enterprise	■ T5440 ■ T5220 ■ T5120 ■ T5140 ■ T5240 ■ T6340
x86 Sun Fire	■ X4140 ■ X4150 ■ X4240 ■ X4440 ■ X4450 ■ X4600 ■ X4600 M2 ■ X4640

Modifying Default Management Access Configuration Properties

Network administrators can optionally accept or modify the default management access properties shipped with Oracle ILOM. To modify the default management access properties in Oracle ILOM, see the following tables:

- [Table 38, “Web Server Configuration Properties,” on page 101](#)
- [Table 39, “SSL Certificate and Private Key Configuration Properties for HTTPS Web Server,” on page 104](#)
- [Table 40, “SNMP Configuration Properties,” on page 107](#)

- Table 41, “SSH Server Configuration Properties,” on page 110
- Table 42, “IPMI Service Configuration Properties,” on page 112
- Table 43, “CLI Session Timeout and Custom Prompt Configuration Properties,” on page 114
- Table 44, “Federal Information Processing Standards (FIPS 140-2) Configuration Properties,” on page 116
- Table 45, “Servicetag Service Configuration Properties,” on page 118

TABLE 38 Web Server Configuration Properties

User Interface Configurable Target and User Role:		
■ CLI: <code>/SP CMM/services/</code> ■ Web: ILOM Administration > Management Access > Web Server > Web Server Settings ■ User Role: admin (a) (required for all property modifications)		
Property	Default Value	Description
HTTP Webserver (http/ securedirect=enabled servicestate=disabled)	Redirect Connection to HTTPS	<i>Redirect Connection to HTTPS Enabled Disabled</i> When the HTTP Webserver property is set to Redirect Connection to HTTPS, the service state property for HTTPS Webserver is automatically enabled. These default property values instruct Oracle ILOM to use HTTPS to securely transmit information to the web server. When the HTTP Webserver property is set to enabled, Oracle ILOM uses HTTP a non-encrypted protocol to transmit information to the web server. When the HTTP Webserver property is set to disabled, the use of the transmitting information to the web server using HTTP is disabled in Oracle ILOM. CLI Syntax for HTTP Web Server: set /SP CMM/services/http securedirect=enabled disabled servicestate=disabled enabled
HTTP Port (http/ port=)	80	<i>80 User_defined</i> When the HTTP service state is enabled, Oracle ILOM by default, communicates with the web server using HTTP over TCP port 80. If necessary, the default port number can be changed. CLI Syntax for HTTP Port: set /SP CMM/services/http port=<n>
HTTP Session Timeout (http/ sessiontimeout=)	15 seconds	<i>15 seconds User_defined</i> The HTTP web session timeout determines how many minutes until an inactive web browser client is automatically logged out. The default HTTP web session timeout is 15 minutes. If necessary, the default session timeout value can be increased or decreased. CLI Syntax for HTTP Session Timeout: set /SP CMM/services/http sessiontimeout=<n>

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/services/`
- Web: **ILOM Administration > Management Access > Web Server > Web Server Settings**
- User Role: **admin (a)** (required for all property modifications)

Property	Default Value	Description
HTTPS Webserver (https/ servicestate=enabled)	Enabled	<i>Enabled Disabled</i> When the HTTPS Webserver property is enabled, Oracle ILOM uses the encrypted protocol HTTPS to securely transmit information. In addition, when this property is enabled, you can enable one or more of the supported encryption protocol properties based on the needs of your network environment. Note - As of Oracle ILOM firmware version 4.0.4, TLS v1.2 is enabled by default. TLS v1.1 is disabled by default. Note - An SSL certificate is required for HTTPS. Oracle ILOM includes a default certificate, or you can upload your own certificate with a matched private key. For more information, see the C “Use of Web Server Certificates and SSH Server-Side Keys” on page 93. When the HTTPS Webserver property is set to disabled, the use of transmitting information to the web server using HTTPS is disabled in Oracle ILOM. Note - If you need to disable the HTTPS service and your system supports the Oracle ILOM Remote System Console Plus, disabling the HTTPS service (port 443) is not enough. For systems supporting the Oracle ILOM Remote System Console Plus, both the HTTPS and KVMS services must be disabled. For systems supporting the Oracle ILOM Remote System Console, you can disable the HTTPS service (port 443) only. CLI Syntax for HTTPS Web Server: set /SP CMM/services/https servicestate=enabled disabled
HTTPS Port (https/ port=)	443	<i>443 User_defined</i> When the HTTPS service state is enabled, Oracle ILOM, by default, communicates with the web server using HTTPS over TCP port 443. If necessary, the default port number can be changed. HTTPS Port CLI Syntax: set /SP CMM/services/https port=<n>
HTTPS Session Timeout (https/ sessiontimeout=)	15 seconds	<i>15 seconds User_defined</i> The HTTPS web session timeout determines how many minutes until an inactive web browser client is automatically logged out. The default HTTPS web session timeout is 15 minutes. If necessary, the default session timeout value can be increased or decreased. CLI Syntax for HTTPS Session Timeout: set /SP CMM/services/https sessiontimeout=<n>
SSLv2 (https/ sslv2=disabled)	Disabled (in older Oracle ILOM firmware versions)	<i>Disabled Enabled</i> Note - In later versions of Oracle ILOM firmware (3.2.4.x, 3.2.5.x, 3.2.6.x and forward), the SSLv2 encryption protocol property is not available for configuration. If an older firmware

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/services/`
- Web: **ILOM Administration > Management Access > Web Server > Web Server Settings**
- User Role: **admin (a)** (required for all property modifications)

Property	Default Value	Description
		version of Oracle ILOM is running on the managed device, disable the SSLv2 property and enable the TLS v1.2 property to ensure secure HTTPS data transmissions. The SSLv2 property is disabled by default. If necessary, the default SSLv2 property can be enabled. CLI Syntax for SSLv2: set <code>/SP CMM/services/https sslv2=disabled enabled</code>
SSLv3 (https/ sslv3=enabled)	Enabled (in older Oracle ILOM firmware versions)	<i>Disabled Enabled (default)</i> Note - Due to a security vulnerability discovered with SSLv3, the SSLv3 property is not available for configuration in later versions of Oracle ILOM firmware (3.2.4.x, 3.2.5.x, 3.2.6.x, and forward). If an older firmware version of Oracle ILOM is running on the managed device, you should disable the SSLv3 property and enable the TLS v1.2 property. For details about SSLv3 vulnerabilities, refer to the Oracle MOS SSLv3 Vulnerability Article. To enable the strongest secure socket layer encryption, Oracle ILOM supports the use of SSLv3 and TLS. CLI Syntax for SSLv3: set <code>/SP CMM/services/https sslv3=enabled disabled</code>
TLS v1.1, and v1.2, (https/tls# =)	TLS v1.2 Enabled	<i>Enabled Disabled</i> Transport Layer Security (TLS) protocols provide communication security over the Internet. Enabled — When the TLS properties are enabled, Oracle ILOM supports the use of the enabled TLS protocol service. However, if the client does not support the enabled protocol, Oracle ILOM permits the client to negotiate and use the strongest (most-secure) client-supported protocol available. Disabled — When a TLS property is disabled, Oracle ILOM is prevented from using the disabled TLS protocol to transmit information. Note - As of Oracle ILOM firmware release 4.0.0, support for TLSv1.0 is removed. As of Oracle ILOM firmware release 4.0.4, TLSv1.1 is disabled by default. Note - If one upgrades from an older Oracle ILOM firmware version to 4.0.4 and chooses to preserve the current firmware configuration, the TLSv1.1 property after the firmware update will continue to use the same setting previously configured. In this case, if the TLSv1.1 property is enabled, you should disable it for security reasons and ensure that only the property for TLS v1.2 is enabled. For more information about TLS encryption protocols, see Internet specifications (RFCs 2246, 4346, 5246) created and published by the Internet Engineering Task Force (IETF). Note - All Java versions support v1.2. However, if a version <i>prior</i> to Java 7u131 is installed, you will need to manually enable TLS v1.2 in the Java Control Panel, or update your system with a later Java version. CLI Syntax for TLSv1:

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/services/`
- Web: ILOM Administration > Management Access > Web Server > Web Server Settings
- User Role: admin (a) (required for all property modifications)

Property	Default Value	Description
		set <code>/SP CMM/services/web(tls1_1= tls1_2=)enabled disabled</code>
Weak Ciphers (https/ weak_ciphers=disabled)	Disabled (in older Oracle ILOM firmware versions)	<i>Disabled Enabled</i> Note - In later versions of Oracle ILOM firmware (3.2.4.x, 3.2.5.x, 3.2.6.x and forward), the weak cipher property is not available for configuration. If an older firmware version of Oracle ILOM is running on the managed device, disable the weak cipher property and enable the TLS encryption protocol property to ensure secure HTTPS data transmissions. The Weak Ciphers property is disabled by default. It might be necessary to enable weak ciphers to support the use of older web browsers. CLI Syntax for Weak Ciphers: set <code>/SP CMM/services/https weak_ciphers=disabled enabled</code>
Save		Web interface – To apply changes made to properties within the Web Server Settings page, you must click Save.

TABLE 39 SSL Certificate and Private Key Configuration Properties for HTTPS Web Server**User Interface Configurable Target, User Role, SSL Certificate Requirement:**

- CLI: `/SP|CMM/services/https/ssl`
- Web: ILOM Administration > Management Access > SSL Certificate > SSL Certificate Upload
- User Role: admin(a) (required for all property modifications)
- Requirement: A valid custom SSL configuration requires the uploading of both the custom certificate and a custom private key.

Property	Default Value	Description
Certificate File Status (certstatus=)	Using Default (No custom certificate or private key loaded)	<i>Default_Certificate Custom_Certificate</i> The Certificate Status property is a read-only property. This property indicates which of the following types of SSL certificates is currently in use by the HTTPS web server: ■ Self-signed default SSL certificate and key provided with Oracle ILOM - or - ■ Custom trusted SSL certificate and private key provided by a trusted Certificate Authority Note – When the default SSL certificate is in use, users connecting to the Oracle ILOM web interface for the first time are notified of the default self-signed certificate and are prompted to accept its use. Users should always verify that the certificate fingerprint appearing in the warning message matches the certificate fingerprint issued by Oracle. For more information about validating the self-signed Default SSL certificate, see “Resolving Warning Messages for Self-Signed SSL Certificate ” on page 216 The default self-signed SSL certificate ensures that all communication between a web browser client and the Oracle ILOM SP (or CMM) is fully encrypted. CLI Syntax to Show Certificate Status:

User Interface Configurable Target, User Role, SSL Certificate Requirement:

- CLI: `/SP|CMM/services/https/ssl`
- Web: ILOM Administration > Management Access > SSL Certificate > SSL Certificate Upload
- User Role: admin(a) (required for all property modifications)
- Requirement: A valid custom SSL configuration requires the uploading of both the custom certificate and a custom private key.

Property	Default Value	Description
show /SP CMM/https/ssl		
Default SSL Certificate Key Size (/default_cert generate_new_cert_keysize =)	3072	2048 3072 (default) 4096 Note - The Default SSL Certificate Key Size is available for configuration as of Oracle ILOM firmware version 3.2.8. By default, the Oracle ILOM Default SSL Certificate is generated with a 3072 bit key size. Optionally, you can change default key size (3072) to either 2048 or 4096. Web interface – Click the Create Default Certificate Key Size list box and select the appropriate key size. Oracle ILOM will use the newly assigned key size the next time the Default SSL Certificate is generated. Note - When the Oracle ILOM properties are reset to defaults, a new Oracle ILOM self-signed SSL Default Certificate is automatically generated. CLI Syntax to Change Default SSL Certificate Key Size: set /SP CMM/https/ssl/default_cert generate_new_cert_keysize=[2048 3072 4096] The newly assigned key size applies the next time the Default SSL Certificate is generated.
Create Default SSL Certificate (default_cert generate_new_cert_action =)	N/A	As of firmware version 3.2.8, each Oracle ILOM SP and CMM ships with a unique self-signed Default SSL Certificate. The Default SSL Certificate is used by Oracle ILOM whenever a custom SSL Certificate is not configured. When necessary, system administrators can choose to regenerate a new self-signed Default SSL Certificate. Each generated self-signed Default SSL Certificate has a unique fingerprint value. To verify that the Default SSL Certificate is valid, ensure that the fingerprint value shown on the self-signed Default SSL Certificate warning message matches the certificate fingerprint value issued by Oracle ILOM. For more information about validating the self-signed Default SSL certificate, see “Resolving Warning Messages for Self-Signed SSL Certificate ” on page 216 Note - The SSL Certificate fingerprint value issued by Oracle ILOM appears on the Oracle ILOM SSL Certificate web page (ILOM Administration > Management Access > SSL Certificates) and the Oracle ILOM SSL Certificate CLI target (<code>show /SP CMM/services/https/ssl/default_cert fingerprint</code>). Note - Oracle ILOM automatically regenerates a self-signed Default SSL Certificate when the Oracle ILOM properties are reset to defaults. Web interface – To regenerate a new self-signed Default SSL Certificate from the web interface, click the Create button in the Default Certificate section of the Management Access > SSL Certificate page. CLI Syntax to Create Default SSL Certificate set /SP CMM/https/ssl/default_cert generate_new_cert_action =true

User Interface Configurable Target, User Role, SSL Certificate Requirement:

- **CLI:** `/SP|CMM/services/https/ssl`
- **Web:** **ILOM Administration > Management Access > SSL Certificate > SSL Certificate Upload**
- **User Role:** admin(a) (required for all property modifications)
- **Requirement:** A valid custom SSL configuration requires the uploading of both the custom certificate and a custom private key.

Property	Default Value	Description
		When a new self-signed Default Certificate is generated, the Oracle ILOM web and KVMS console user connections are lost. When this occurs, log in to Oracle ILOM to confirm that a new Default SSL Certificate and fingerprint was generated. For detailed instructions for regenerating a Default SSL Certificate, see “Regenerate Self-Signed Default SSL Certificate Issued By Oracle” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x.
Custom Certificate Load (/ custom_certificate)		Web interface – Click the Load Certificate button to upload the Custom Certificate file that is designated in the File Transfer Method properties. Note. A valid custom certificate configuration requires the uploading of a custom certificate and a custom private key. Only then will the custom SSL certificate configuration apply and be persistent across system reboots and Backup and Restore operations. CLI Syntax to Load Custom Certificate: load_uri=file_transfer_method://host_address/file_path/custom_certificate_filename Where <i>file_transfer_method</i> can include: <i>Browser TFTP FTP SCP HTTP HTTPS Paste</i> For a detailed description of each file transfer method (excluding Paste), see “Supported File Transfer Methods” on page 50 For additional information about using a custom signed SSL Certificate in Oracle ILOM, see “Improve Security by Using a Trusted SSL Certificate and Private Key” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x. Note - If a custom certificate and private key are not properly configured, Oracle ILOM, as of firmware 3.2.10, will generate a warning message. For further details, see “Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate” on page 218 Note - When using a certificate chain, ensure that the certificates in the certificate chain file are in the correct order. For more details, see "Certificate Chain Order" under “Upload a Custom SSL Certificate and Private Key to Oracle ILOM” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x.
Custom Certificate Remove (/custom_certificate clear_action=true)		Web interface – Click the Remove Certificate Button to remove the Custom SSL Certificate file presently stored in Oracle ILOM. When prompted, click Yes to delete or No to cancel action. CLI Syntax to Remove Certificate: set /SP CMM/services/https/ssl/custom_certificate clear_action=true When prompted, type y to delete or n to cancel action.
Custom Private Key		Web interface – Click the Load Custom Private Key button to upload the Custom Private Key file that is designated in the File Transfer Method properties.

User Interface Configurable Target, User Role, SSL Certificate Requirement:

- CLI: `/SP|CMM/services/https/ssl`
- Web: **ILOM Administration > Management Access > SSL Certificate > SSL Certificate Upload**
- User Role: **admin(a)** (required for all property modifications)
- Requirement: A valid custom SSL configuration requires the uploading of both the custom certificate and a custom private key.

Property	Default Value	Description
<code>(/custom_key)</code>		Note. A valid custom certificate configuration requires the uploading of a custom certificate and a custom private key. Only then will the custom SSL certificate configuration apply and be persistent across system reboots and Backup and Restore operations. CLI Syntax to Load Custom Private Key: <code>load_uri=file_transfer_method://host_address/file_path/custom_key_filename</code> Where <i>file_transfer_method</i> can include: <i>Browser TFTP FTP SCP HTTP HTTPS PasteFor</i> a detailed description of each file transfer method (excluding Paste), see “Supported File Transfer Methods” on page 50. For additional information about using a custom signed SSL Certificate in Oracle ILOM, see “Improve Security by Using a Trusted SSL Certificate and Private Key” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x.
Custom Private Key Remove <code>(/custom_key clear_action=true)</code>		Web interface – Click the Remove Custom Private Key button to remove the Custom Private Key file presently stored in Oracle ILOM. When prompted, click Yes to delete or No to cancel the action. CLI Syntax to Remove Certificate Private Key: <code>set /SP CMM/services/https/ssl/custom_key clear_action=true</code> When prompted, type y to delete or n to cancel the action.

TABLE 40 SNMP Configuration Properties**User Interface Configurable Target, User Role, and SNMP Requirement:**

- CLI: `/SP|CMM/services/snmp`
- Web: **ILOM Administration > Management Access > SNMP > SNMP Management**
- User Role: **admin (a)** (required for all property modifications)
- Requirement: User accounts are required for SNMPv3 service; Communities are required for SNMPv1 or v2c service.

Property	Default Value	Description
State <code>(state=)</code>	Enabled	<i>Enabled Disabled</i> The SNMP State property is enabled by default. When this property is enabled, and the properties for one or more user accounts or communities for SNMP are configured, the SNMP management service in Oracle ILOM is available for use. When the SNMP State property is disabled, the SNMP port is blocked, prohibiting all SNMP communication between Oracle ILOM and the network. CLI Syntax for SNMP State: <code>set /SP CMM/services/snmp state=enabled disabled</code>

User Interface Configurable Target, User Role, and SNMP Requirement:

- **CLI:** `/SP|CMM/services/snmp`
- **Web:** **ILOM Administration > Management Access > SNMP > SNMP Management**
- **User Role:** **admin (a)** (required for all property modifications)
- **Requirement:** **User accounts are required for SNMPv3 service; Communities are required for SNMPv1 or v2c service.**

Property	Default Value	Description
Port (port=)	161	<i>161 User_specified.</i> Oracle ILOM, by default, uses UDP port 161 to transmit SNMP communication between an Oracle ILOM SP (or Oracle ILOM CMM) and the network. If necessary, the default port property number can be changed. CLI Syntax for SNMP Port: set /SP CMM/services/snmp port=<i>n</i>
Engine ID (engineid=)	Auto-set by SNMP agent	The Engine ID property is automatically set by the Oracle ILOM SNMP agent. This ID is unique to each Oracle ILOM SNMP enabled-system. Although the Engine ID is configurable, the ID should always remain unique across the data center for each Oracle ILOM system. Only experienced SNMP users who are familiar with SNMP v3 security should modify the SNMP Engine ID property.
Set Requests (sets=)	Disabled	<i>Disabled Enabled</i> The Set Requests property is disabled in Oracle ILOM by default. When the Sets Requests property is disabled, the following SNMP MIBs are available for monitoring purposes: ■ SUN-HW-TRAP-MIB – Use this MIB to monitor trap notifications for hardware-related events such as faults. ■ SUN-PLATFORM-MIB – Use this MIB to poll hardware-related information such as inventory and health. When the Set Requests property is enabled, the MIBs described above are available for monitoring purposes and the following MIBs are available for management purposes: ■ SUN-HW-CTRL-MIB – Use this MIB to configure hardware policies such as power management. ■ SUN-ILOM-CONTROL-MIB – Use this MIB to configure Oracle ILOM features such as creating users and configuring services. CLI Syntax for Set Requests: set /SP CMM/services/snmp sets=<i>disabled enabled</i> Related Information: ■ “Configuring SNMP Settings in Oracle ILOM” in Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x
Protocols (v1 v2c v3)	v3, Enabled	<i>v1 v2c v3</i> Oracle ILOM, by default, enables the use of SNMP v3 and disables the use of SNMP v1 and v2c.

User Interface Configurable Target, User Role, and SNMP Requirement:

- CLI: `/SP|CMM/services/snmp`
- Web: ILOM Administration > Management Access > SNMP > SNMP Management
- User Role: admin (a) (required for all property modifications)
- Requirement: User accounts are required for SNMPv3 service; Communities are required for SNMPv1 or v2c service.

Property	Default Value	Description
		SNMPv1 and v2c do not support encryption and use community strings as a form of authentication. SNMPv3 uses encryption to provide a secure channel and uses individual user names and passwords that are stored securely on the SNMP management station. If necessary, the default SNMP Protocol property value is configurable. Note - Use SNMP v2c or v3 for monitoring purposes and keep the default property disabled for Set Requests. CLI Syntax to Modify Default Protocol: set <code>/SP CMM/services/snmp v1 v2c v3=enabled disabled</code>
Save		Web interface – To apply changes made to properties within the SNMP Management page, you must click Save.
SNMP Communities (/communities)		<i>Community Name</i> <i>Permission= Read-only (ro) Read-write (rw)</i> SNMP communities apply only to SNMP v1 or v2c to control user access and authorization levels in Oracle ILOM. When the Protocols property for SNMP v1 or v2c is enabled, the properties for SNMP communities are configurable in Oracle ILOM. The following rules apply when configuring communities: ■ Community name – Up to 35 characters in length, must start with an alphabetic character, and must not contain any spaces ■ Save (web interface only) – All changes made within the SNMP Add SNMP User dialog must be saved CLI Syntax to Create SNMP Communities: create <code>/SP CMM/services/snmp/communities name=community_name permission=rw ro</code> show <code>/SP CMM/services/snmp/communities public private</code> delete <code>/SP CMM/services/snmp/communities community_name</code>
SNMP Users (/users)		<i>Username</i> <i>Authentication Password</i> <i>Permission</i> <i>Authentication Protocol</i> <i>Privacy Protocol</i> SNMP Users apply only to SNMP v3 to control user access and authorization levels in Oracle ILOM. When the Protocol property for SNMP v3 is enabled, the properties for SNMP users are configurable in Oracle ILOM. The following rules apply when configuring SNMP users: ■ User name – The SNMP user name can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers). The SNMP user name must <i>not</i> contain spaces.

User Interface Configurable Target, User Role, and SNMP Requirement:

- **CLI:** `/SP|CMM/services/snmp`
- **Web:** ILOM Administration > Management Access > SNMP > SNMP Management
- **User Role:** admin (a) (required for all property modifications)
- **Requirement:** User accounts are required for SNMPv3 service; Communities are required for SNMPv1 or v2c service.

Property	Default Value	Description
		■ Authentication or privacy password – The Authentication password can contain 8 to 12 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers). ■ Privacy password – Enter the privacy password (required only if you selected @ DES or AES). The password is case-sensitive and must contain 8 characters in length with no colons or spaces. ■ Save (web interface only – All changes made within the SNMP Add SNMP User dialog must be saved. CLI Syntax to Create SNMP Users: <pre>create /SP CMM/services/snmp/users/[new_username] authenticationprotocol=[MD5 SHA] authenticationpassword=[changeme] permission=[ro rw] privacyprotocol=[AES DES none] privacypassword=[user_password]</pre> <pre>show /SP CMM/services/snmp/users</pre> <pre>delete /SP CMM/services/snmp/username</pre> Note - Authentication Protocol MD5 and DES Privacy Protocol are not supported when FIPS compliance mode is enabled in Oracle ILOM.
MIBs Download (/mibs dump_uri=)		Oracle ILOM provides the ability to download SUN SNMP MIBs directly from the server SP or CMM.

TABLE 41 SSH Server Configuration Properties**User Interface Configurable Target and User Role:**

- **CLI:** `/SP|CMM/services/ssh`
- **Web:** ILOM Administration > Management Access > SSH Server > SSH Server Settings
- **User Role:** admin (a) (required for all property modifications)

Property	Default Value	Description
State (state=)	Enabled	<i>Enabled Disabled</i> The SSH Server State property is enabled by default. When the SSH Server State property is enabled, the SSH server uses server-side keys to permit remote clients to securely connect to the Oracle ILOM SP (or Oracle ILOM CMM) using a command-line interface.

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/services/ssh`
- Web: ILOM Administration > Management Access > SSH Server > SSH Server Settings
- User Role: admin (a) (required for all property modifications)

Property	Default Value	Description
		When the SSH Server State property is disabled or restarted, all CLI SP or CLI CMM sessions running over SSH are automatically terminated. Note - Oracle ILOM automatically generates the SSH server-side keys on the first boot of a factory default system. Web interface: Changes to the SSH Server State in the web interface do not take affect in Oracle ILOM until you click Save. Note - Changes to the SSH Server State property do <i>not</i> require you to restart the SSH server. CLI Syntax for SSH Server State: set <code>/SP CMM/services/ssh state=enabled disabled</code>
Weak Ciphers (weak_ciphers=)	Disabled (in earlier versions of Oracle ILOM firmware 3.2.5)	<i>Enabled</i> <i>Disabled</i> Note - Due to security vulnerabilities, the weak cipher property for SSH should be disabled. This property is no longer available for configuration in later firmware versions of Oracle ILOM (3.2.5.x, 3.2.6.x, and forward). The Weak Ciphers property controls whether the Weak Ciphers mode for the Oracle ILOM SSH Server is enabled. ■ Disabled (default) — When the SSH Weak Ciphers mode is disabled, the Oracle ILOM SSH Server prevents remote SSH clients from using a weaker cipher suite (weaker encryption) to transmit sensitive information. ■ Enabled — When the SSH Weak Ciphers mode is enabled, the Oracle ILOM SSH Server permits remote SSH clients to negotiate a weaker cipher suite (weaker encryption) to transmit sensitive information. This option is best used in private intranet environments. Web interface: Changes to the SSH Weak Ciphers property in the web interface do not take affect until you click Save. Note - Changes to the Weak Ciphers property do <i>not</i> require you to restart the SSH server. The change takes affect immediately on all new SSH connections. CLI Syntax for SSH Weak Ciphers: set <code>/SP CMM/services/ssh weak_ciphers=enabled disabled</code>
Restart Button (restart_sshd_action=)		<i>True</i> <i>False</i> Restarting the SSH server will automatically: (1) terminate all connected SP or CMM CLI sessions, as well as (2) activate newly pending server-side key(s).

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/services/ssh`
- Web: ILOM Administration > Management Access > SSH Server > SSH Server Settings
- User Role: admin (a) (required for all property modifications)

Property	Default Value	Description
CLI Syntax for Restart:		
set /SP CMM/services/ssh restart_sshd_action=true		
Generate RSA Key Button (generate_new_key_type=rsa generate_new_key_action= true)		Provides the ability to generate a new RSA SSH key. CLI Syntax for Generate RSA Key: set /SP CMM/services/ssh generate_new_key_type=rsa generate_new_key_action=true
Generate DSA Key Button (generate_new_key_type=dsa generate_new_key_action=)		Provides the ability to generate a new DSA SSH key. CLI Syntax for Generate DSA Key: set /SP CMM/services/ssh generate_new_key_type=dsa generate_new_key_action=true

TABLE 42 IPMI Service Configuration Properties**User Interface Configurable Target:**

- CLI: `/SP|CMM/services/ipmi`
- Web: ILOM Administration > Management Access > IPMI > IPMI Settings

User Roles:

- admin (a) – Required for IPMI specification configuration property modifications
- Administrator or Operator – Required when using IPMI service (IPMITool) from the Oracle ILOM CLI.

Property	Default Value	Description
State (state=)	Enabled	<i>Enabled (default) Disabled</i> As of Oracle ILOM firmware version 3.2.8, the State property for IPMI TLS service is enabled by default. Prior to Oracle ILOM firmware version 3.2.8, the State property for IPMI 2.0 is disabled by default. When the IPMI State property is enabled, Oracle ILOM permits remote IPMITool clients to securely connect to the Oracle ILOM SP (or Oracle ILOM CMM) using a command-line interface. When the IPMI State property is disabled, all IPMITool clients connected to the SP or CMM through the Oracle ILOM CLI are automatically terminated.

User Interface Configurable Target:

- CLI: `/SP|CMM/services/ipmi`
- Web: **ILOM Administration > Management Access > IPMI > IPMI Settings**

User Roles:

- **admin (a)** – Required for IPMI specification configuration property modifications
- **Administrator or Operator** – Required when using IPMI service (IPMITool) from the Oracle ILOM CLI.

Property	Default Value	Description
v1.5 Sessions (v1_5_sessions=)	Disabled	Web interface: Changes to the IPMI State in the web interface do not take affect in Oracle ILOM until you click Save. CLI Syntax for IPMI State: set <code>/SP CMM/services/ipmi state=enabled disabled</code> <i>Enabled Disabled (default)</i> Note - By default, Oracle ILOM supports the use of the IPMI v2.0 service and the TLS service. P As of Oracle ILOM firmware release 3.2.4, a configurable sessions property for the IPMI v1.5 service is provided. By default, the v1.5 Sessions property is disabled. When the v1.5 Sessions property is disabled, all remote IPMITool clients using the IPMI v1.5 service are prevented from connecting to Oracle ILOM. When the v1.5 Sessions property is enabled, Oracle ILOM permits remote IPMITool clients using the IPMI v1.5 service to connect to the Oracle ILOM SP (or Oracle ILOM CMM) using a command-line interface. Web interface: Changes to the IPMI State in the web interface do not take affect in Oracle ILOM until you click Save. CLI Syntax for v1.5 Sessions: set <code>/SP CMM/services/ipmi v1_5_sessions=enabled disabled</code> Note - When FIPS mode is enabled in Oracle ILOM, the non-compliant FIPS 140-2 IPMI v1.5 Sessions property is removed from Oracle ILOM interfaces and is not available for configuration. For additional information about securing Oracle ILOM when using an IPMI service to manage Oracle servers, see the IPMI topics in the <i>Oracle ILOM Security Guide</i>.
v2.0 Sessions (v1_5_sessions=)	Enabled	<i>Enabled (default) Disabled</i> When the v2.0 Sessions property is disabled, all remote IPMITool clients using the IPMI v2.0 service are prevented from connecting to Oracle ILOM. When the v2.0 Sessions property is enabled, Oracle ILOM permits remote IPMITool clients using the IPMI v1.5 service to connect to

User Interface Configurable Target:

- CLI: `/SP|CMM/services/ipmi`
- Web: ILOM Administration > Management Access > IPMI > IPMI Settings

User Roles:

- admin (a) – Required for IPMI specification configuration property modifications
- Administrator or Operator – Required when using IPMI service (IPMITool) from the Oracle ILOM CLI.

Property	Default Value	Description
TLS Sessions (tls_sessions=)	Enabled	the Oracle ILOM SP (or Oracle ILOM CMM) using a command-line interface. Web interface: Changes to the IPMI State in the web interface do not take affect in Oracle ILOM until you click Save. CLI Syntax for v1.5 Sessions: set <code>/SP CMM/services/ipmi v2_0_sessions=enabled disabled</code> <i>Enabled (default) Disabled</i> As of Oracle ILOM firmware version 3.2.8, the TLS sessions (tls_sessions) property is enabled by default. To disable TLS sessions, you must disable the IPMI State property. For increased security, always use the TLS service and interface. Note - IPMI TLS is an Oracle improvement to IPMI security which requires a special version of the ipmitool client that supports TLS sessions For more information about using the TLS service and interface, see the following information: ■ “IPMI TLS Service and Interface” in Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x ■ “Configure IPMI Management Access for Increased Security” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x

TABLE 43 CLI Session Timeout and Custom Prompt Configuration Properties**User Interface Configurable Target:**

- CLI: `/SP|CMM/cli`
- Web: ILOM Administration > Management Access> CLI

User Roles:

- admin (a) – Required for IPMI specification configuration property modifications
- Administrator or Operator – Required when using IPMI service (IPMITool) from the Oracle ILOM CLI.

Property	Default Value	Description
Session Timeout (timeout=)	Disabled	<i>Disabled Enabled, minutes=n</i>

User Interface Configurable Target:

- CLI: `/SP|CMM/cli`
- Web: **ILOM Administration > Management Access > CLI**

User Roles:

- **admin (a)** – Required for IPMI specification configuration property modifications
- **Administrator or Operator** – Required when using IPMI service (IPMITool) from the Oracle ILOM CLI.

Property	Default Value	Description
		The CLI Session Timeout property determines how many minutes until an inactive CLI session is automatically logged out. By default, there is no CLI timeout configured. If the Oracle ILOM CLI is used on a shared console, network administrators are recommended to set the CLI session timeout value to 15 minutes or less. Web interface: Changes to the CLI session timeout properties in the web interface do not take affect in Oracle ILOM until you click Save. CLI Syntax for CLI Session Timeout: set <code>/SP CMM/cli timeout=enabled disabled</code> minutes=<i>value</i>
Custom Prompt (prompt=)	None (disabled)	<i>None (default) ["Literal Text"] "<HOSTNAME>" "<IPADDRESS>"</i> To help identify a standalone system or a system within a rack or chassis, Administrators can customize the standard CLI

Note - The Custom CLI Prompt feature is initially available for configuration on Oracle

User Interface Configurable Target:

- CLI: `/SP|CMM/cli`
- Web: ILOM Administration > Management Access > CLI

User Roles:

- admin (a) – Required for IPMI specification configuration property modifications
- Administrator or Operator – Required when using IPMI service (IPMITool) from the Oracle ILOM CLI.

Property	Default Value	Description
Network OPUS Switches as of firmware release 3.2.5.x.		prompt (->) by prepending either literal text, replacement tokens ("<code><HOSTNAME></code>" "<code><IPADDRESS></code>"), or a combination of literal text and replacement tokens. The Custom Prompt maximum length is 252 characters. Web interface: Changes to the CLI Custom Prompt property in the web interface do not take affect in Oracle ILOM until you click Save. For further information, click the <i>More details...</i> link on the Management Access > CLI page. CLI Syntax for Custom CLI Prompt: Examples: ■ <code>set /SP CMM FMM/cli prompt="Literal_Text"</code> ■ <code>set /SP CMM FMM/cli prompt="<HOSTNAME>"</code> ■ <code>set /SP CMM FMM/cli prompt="<IPADDRESS>"</code> ■ <code>set /SP CMM FMM/cli prompt=["Literal_Text"] "<HOSTNAME>"</code> ■ <code>set /SP CMM FMM/cli prompt=["Literal_Text"] "<HOSTNAME>" "<IPADDRESS>"</code>

TABLE 44 Federal Information Processing Standards (FIPS 140-2) Configuration Properties**User Interface Configurable Target and User Role:**

- CLI: `/SP/services/fips`
- Web: ILOM Administration > Management Access > FIPS
- User Role: admin (a) (required for property modification)

Property	Default Value	Description
Status (status=)	Disabled	The Status is a read-only property that indicates the current status for the FIPS service in Oracle ILOM. Possible status values are: ■ Disabled — The Status for <i>Disabled</i> appears on the Management Access > FIPS page when the following conditions are true: 1. The FIPS operational mode on the system is disabled. 2. The State property is set to disabled. 3. The FIPS shield icon <i>does not</i> appear in the masthead area of the Oracle ILOM window.

User Interface Configurable Target and User Role:

- CLI: `/SP/services/fips`
- Web: **ILOM Administration > Management Access > FIPS**
- User Role: **admin (a)** (required for property modification)

Property	Default Value	Description
		■ Enabled — The Status for <i>Enabled</i> appears on the Management Access > FIPS page when the following conditions are true: 1. The FIPS operational mode on the system is enabled. 2. The State property is set to enabled. 3. The FIPS shield icon appears in the masthead area of the Oracle ILOM window. ■ Disabled; enabled at next boot — The Status for <i>Disabled; enabled at next boot</i> appears on the Management Access > FIPS page when the following conditions are true: 1. The FIPS operational mode on the system is disabled. 2. The State property is set to enabled. 3. The FIPS shield icon <i>does not</i> appear in the masthead area of the Oracle ILOM window. ■ Enabled; disabled at next boot — The Status for <i>Enabled; disabled at next boot</i> appears on the Management Access > FIPS page when the following conditions are true: 1. The FIPS operational mode on the system is enabled. 2. The State property is set to disabled. 3. The FIPS shield icon appears in the masthead area of the Oracle ILOM window.

Related Information:

- [“Operating Oracle ILOM in FIPS Compliance Mode” on page 89](#)
- [“Unsupported Features When FIPS Mode Is Enabled” on page 92](#)

State (state=disabled enabled)	Disabled	Modify the FIPS State property, per the following instructions: ■ To disable FIPS mode (default) — Select the State check box to disable FIPS compliant mode. ■ To enable FIPS mode — Clear the State check box to enable FIPS compliant mode. Changes to the FIPS operational mode on the server will not take effect until the next Oracle ILOM reboot. At that time, the Oracle ILOM user-defined configurations settings are automatically reset to their factory default settings.
---	----------	--

CLI Syntax for FIPS Mode:

```
set /SP/services/fips state=enabled|disabled
```

Related Information:

- [“Modify FIPS Mode ” on page 89](#)

User Interface Configurable Target and User Role:

- CLI: `/SP/services/fips`
- Web: ILOM Administration > Management Access > FIPS
- User Role: admin (a) (required for property modification)

Property	Default Value	Description
		■ “FIPS Compliance Mode Effect on ILOM Configuration Properties” on page 91

TABLE 45 Servicetag Service Configuration Properties**User Interface Configurable Target and User Role:**

- CLI: `/SP/services`
- User Role: admin (a) (required for all property modifications)

Property	Default Value	Description
servicetag=	Enabled	<i> Enabled (default) Disabled</i> The servicetag service is enabled by default. When enabled, the Oracle discovery protocol is used to identify servers and facilitate service requests. Disabling this service makes it impossible for Oracle Enterprise Manager Ops Center to discover Oracle ILOM, and prevents integration into other Oracle automatic service solutions. Caution - The servicetag service uses HTTP by default as a communication method. To protect sensitive data, configure the servicetag property with a passphrase and use HTTPS as a communication method. Note - The servicetag property is only configurable from Oracle ILOM CLI. CLI Syntax for Servicetag: set /SP/services/servicetag= <i>disabled enabled</i>
passphrase=	user-defined	To encrypt servicetag data, set a value for the servicetag passphrase property. Note - The matching service tag value should be entered in the Oracle Service Solution program such as ASR or the original Java Service Tag program. CLI Syntax for Passphrase: set /SP/services/passphrase=<value> The passphrase length must be between 5 and 16 characters.

Modifying Default Connectivity Configuration Properties

Network administrators can optionally accept or modify the default connectivity properties shipped with Oracle ILOM. To modify the default connectivity properties in Oracle ILOM, see the following tables:

- [Table 46, “Network Connectivity Standard Configuration Properties ,” on page 119](#)
Network Connectivity Standard Configuration Properties

Note - The standard IP properties include instructions to independently enable or disable network connectivity for an IPv4 environment or a dual-stack (IPv4 and IPv6) environment.

- [Table 47, “Network Connectivity Enhanced Configuration Properties ,” on page 126](#)
Network Connectivity Enhanced Configuration Properties

Note - As of Oracle ILOM 3.2.4, the IP settings were enhanced to independently enable or disable the property States for IPv4 and IPv6 network connectivity. In addition, a new static IPv6 gateway property is available for configuration. These enhanced settings are available on most new server models, and a select number of legacy servers running a later software release.

- [Table 48, “DNS Configuration Properties ,” on page 134](#)
- [Table 49, “Serial Port Configuration Properties ,” on page 136](#)

Note - For Oracle's multi-domain SPARC servers, refer to the server administration guide for detailed information about how to configure connectivity properties in Oracle ILOM.

TABLE 46 Network Connectivity Standard Configuration Properties

User Interface Configurable Target and User Role:		
■ CLI: <code>/SP CMM/network</code> ■ Web: ILOM Administration > Connectivity > Network > Network Settings ■ User Role: admin (a) (required for all property modifications)		
Requirements:		
■ Standard connectivity configuration properties apply to all servers running Oracle ILOM 3.2.0, 3.2.1, 3.2.2, and 3.2.3. They also apply to some server models running Oracle ILOM firmware 3.2.4 and later. Refer your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system. ■ All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made in the Network Settings page must be saved to take affect in Oracle ILOM.		
Property	Default Value	Description
State (state=)	Enabled	<i>Enabled Disabled</i> The network State property is enabled by default. This property must always be enabled in order for Oracle ILOM to operate in an IPv4 network environment or in a dual-stack IPv4 and IPv6 network environment. CLI Syntax to Set Network State: set <code>/SP CMM/network state=enabled disabled</code>
MAC Address	Read-only	<code>macaddress= outofbandaddress= sidebandmacaddress=</code>

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: ILOM Administration > Connectivity > Network > Network Settings
- User Role: admin (a) (required for all property modifications)

Requirements:

- Standard connectivity configuration properties apply to all servers running Oracle ILOM 3.2.0, 3.2.1, 3.2.2, and 3.2.3. They also apply to some server models running Oracle ILOM firmware 3.2.4 and later. Refer your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made in the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
Out of Band MAC Address		The media access control (MAC) addresses for the server SP and CMM are set at the factory.
Sideband MAC Address		The MAC Address properties for both the SP and CMM are non-configurable read-only properties in Oracle ILOM.
CLI Syntax to Show MAC Address Properties: show /SP CMM/network		
Management Port (managementport=)	MGMT	<i>MGMT NETn</i> All servers shipped with Oracle ILOM include a physical network management port (MGT) used for connecting to Oracle ILOM over a network. Some systems shipped with Oracle ILOM also support sideband management. Sideband management shares the use of a physical data port (NETn) on the server to permit network access to both the host operating system and Oracle ILOM. For systems supporting this option, network administrators can either choose to accept the default Management Port property (MGMT) or modify the Management Port property for sideband management use (NETn). CLI Syntax for SP Management Port: set /SP/network pendingmanagementport=MGMT NETn set /SP CMM/network commitpending=true Related Information: ■ “Sideband Network Management Connection” on page 20 ■ “Dedicated Network Management Connection (Default)” on page 18
VLAN Tag (pendingvlan_id=)	(none)	<i>Integer between 1 and 4079</i> In Oracle ILOM, VLAN tagging is disabled by default. While VLAN tagging is disabled, the system does not generate VLAN-tagged Ethernet frames and does not process incoming VLAN-tagged Ethernet frames. If you enable VLAN tagging, the system can generate and receive VLAN-tagged Ethernet frames in accordance with the Institute of Electrical and Electronics Engineers (IEEE) 802.1Q standard. Specify the VLAN tag as an integer between 1 and 4079. Alternatively, use a VLAN Tag value of 0 in the web interface or “” in the CLI to disable VLAN tagging.

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: **ILOM Administration > Connectivity > Network > Network Settings**
- User Role: admin (a) (required for all property modifications)

Requirements:

- Standard connectivity configuration properties apply to all servers running Oracle ILOM 3.2.0, 3.2.1, 3.2.2, and 3.2.3. They also apply to some server models running Oracle ILOM firmware 3.2.4 and later. Refer your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made in the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
CLI Syntax for VLAN Tag:		
<pre>set /SP/network pendingvlan_id=[1-4079 ""] commitpending=true</pre>		
IPv4 IP Discovery Mode (ipdiscovery=)	DHCP	<i>DHCP Static</i> The property for IPv4 Discovery Mode in Oracle ILOM is set to DHCP by default. When this property is set to DHCP, Oracle ILOM uses DHCP to determine the physical network address for the server SP or CMM. Optionally, network administrators can disable the DHCP property and choose to configure a static IPv4 network address, Netmask address and Gateway address for the server SP or CMM. Note. When DHCP is set, Oracle ILOM uses the default Auto DNS property to assign the DNS named server and search path. For dual-stack DHCP configurations, the DNS settings in Oracle ILOM can be set to receive DNS information from either the IPv4 or the IPv6 DHCP server. CLI Syntax for IPv4 IP Discovery Mode: <pre>set /SP CMM/network pendingipdiscovery=dhcp static set /SP CMM/network commitpending=true</pre> Related Information: ■ Table 48, “DNS Configuration Properties,” on page 134
IPv4	None	<i>None SysID</i> The property for the DHCP Client ID is set to None by default. Optionally, network administrators can set a SysID (System Identifier) for the DHCP Client using the <code>system_identifier</code> property under the <code>/SP</code> target. CLI Syntax for IPv4 DHCP Client ID: <pre>show /SP CMM/network dhcp_clientid=none sysid</pre> Related Information: ■ “Assigning System Identification Information” on page 140

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: ILOM Administration > Connectivity > Network > Network Settings
- User Role: admin (a) (required for all property modifications)

Requirements:

- Standard connectivity configuration properties apply to all servers running Oracle ILOM 3.2.0, 3.2.1, 3.2.2, and 3.2.3. They also apply to some server models running Oracle ILOM firmware 3.2.4 and later. Refer your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made in the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
IPv4	Static IP	ipaddress= ipnetmask= ipgateway= Note - IP addresses in the following subnets are reserved and cannot be assigned: 169.254.10.n, 169.254.11.n, 169.254.12.n The IP4 user-configurable address properties for Network, Netmask, and Gateway are disabled in Oracle ILOM by default. Optionally, network administrators can set a Static value for the IP Discovery Mode property and manually populate the static IPv4 addresses for Network, Netmask and Gateway. CLI Syntax for IPv4 Static Addresses: <pre>set /SP CMM/network pendingipaddress=value pendingipnetmask=value pendingipgateway=value</pre> <pre>set /SP CMM/network commitpending=true</pre> Related Information: ■ “Input Format for IPv4 and IPv6 Addresses” on page 98
Network Address	Discovery Mode, Disabled	
Netmask Address		
Gateway Address		
IPv6	Enabled	<i>Enabled Disabled</i> The IPv6 State property is enabled in Oracle ILOM by default. Optionally, network administrators can disable the IPv6 network state for any network environment that is not dependent on a dual-stack IP network connection. Note – The IPv6 state must be enabled in Oracle ILOM to support a dual-stack IP network connection. ICLI Syntax for IPv6 State: <pre>set /SP CMM/network/ipv6 state=enabled disabled</pre>
State (/ipv6/ state=)		
IPv6 Autoconfig	Stateless	<i>disabled stateless</i> The IPv6 Autoconfig property is set to Stateless in Oracle ILOM by default. When the Autoconfig Stateless property is enabled, Oracle ILOM learns its IPv6 dynamic address prefixes from the IPv6 router. When the IPv6 Autoconfig Stateless property is set to Disabled, the ability for IPv6 Autoconfig is disabled.
(/ipv6 autoconfig=)		

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: **ILOM Administration > Connectivity > Network > Network Settings**
- User Role: **admin (a)** (required for all property modifications)

Requirements:

- Standard connectivity configuration properties apply to all servers running Oracle ILOM 3.2.0, 3.2.1, 3.2.2, and 3.2.3. They also apply to some server models running Oracle ILOM firmware 3.2.4 and later. Refer your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made in the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
Special Considerations:		
■ The IPv6 Autoconfig Stateless options determine the IP address without any IP support from a DHCPv6 server. ■ The IPv6 Autoconfig Stateless property can be enabled in Oracle ILOM regardless of how the property for DHCPv6 Autoconfig is set.		
CLI Syntax for IPv6 Autoconfig:		
set <code>/SP CMM/network/ipv6 autoconfig=stateless disabled</code>		
DHCPv6 Autoconfig (/ipv6 autoconfig=)	(none)	<i>DHCPv6_Stateless DHCP_Stateful</i> The DHCPv6 Autoconfig property is disabled in Oracle ILOM by default. When this property is disabled, Oracle ILOM is prevented from learning the SP or CMM network addresses and DNS information from a DHCPv6 server on the network. Optionally, network administrators can choose to enable the DHCPv6 Autoconfig property by setting one of the following property values: ■ DHCPv6 Stateless – When enabled, Oracle ILOM automatically learns the DNS information for the server SP (or CMM) from the DHCPv6 network router. ■ DHCPv6 Stateful – When enabled, Oracle ILOM automatically learns the dynamic IPv6 addresses and the DNS information for the server SP (or CMM) from the DHCPv6 network router. Special Considerations: ■ For dual-stack DHCP configurations, the DNS settings in Oracle ILOM can be set to receive DNS information from either the IPv4 or the IPv6 DHCP server. ■ The unique ID for the DHCPv6 server that was last used by Oracle ILOM to retrieve the DHCPv6 network information is identified by the <code>dhcpv6_server_duid</code> property. CLI Syntax for DHCPv6 Autoconfig: set <code>/SP CMM/network/ipv6 autoconfig=dhcpv6_stateless dhcpv6_stateful</code>

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: ILOM Administration > Connectivity > Network > Network Settings
- User Role: admin (a) (required for all property modifications)

Requirements:

- Standard connectivity configuration properties apply to all servers running Oracle ILOM 3.2.0, 3.2.1, 3.2.2, and 3.2.3. They also apply to some server models running Oracle ILOM firmware 3.2.4 and later. Refer your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made in the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
Link-Local IPv6 Address (<code>/ipv6 link_local_ipaddress=</code>)	Read-only	The read-only property for Link-Local IPv6 Address is a non-routable address that you can use to connect to the Oracle ILOM SP (or the CMM) from another IPv6-enabled node on the same network. Oracle ILOM applies the following principles to build the Link-Local Address for the SP or CMM: ■ Oracle ILOM uses the SP or CMM MAC address in conjunction with the link-local identifier prefix. ■ Oracle ILOM, at initialization, uses the Duplicate Address Detection (DAD) protocol to ensure that the reported Local-Link address for the SP (or CMM) is unique. CLI Syntax for Link-Local Address: show <code>/SP CMM/network/ipv6</code>
IPv6 Static IP Address (<code>/ipv6 static_ipaddress=</code>)	None	When the IPv6 state is enabled, network administrators can optionally assign a static IPv6 address to the SP or CMM. Note - IP addresses in the following subnets are reserved and cannot be assigned: 169.254.10.n, 169.254.11.n, 169.254.12.n The parameters for specifying the IPv6 static IP and netmask are: <i>IPv6_address/subnet_mask_length_in_bits</i>. The gateway address, is automatically configured. Example: fec0:a:8:b7:214:4fff:feca:5f7e/64 CLI Syntax for Static IPv6 Address: set <code>/SP CMM/network/ipv6</code> pending_static_ipaddress=ipaddress/subnetmask set <code>/SP CMM/network</code> commitpending=true
IPv6 Gateway (<code>/ipv6 ipgateway=</code>)	Read-only	The read-only IPv6 gateway address presented in this property is learned from an IPv6 router on the network. CLI Syntax for IPv6 Gateway: show <code>/SP CMM/network/ipv6</code>
Dynamic IPv6 Address (<code>/ipv6 dynamic_ipaddress_n</code>)	Read-only	Oracle ILOM reports dynamic IPv6 addresses when the following occurs:

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: **ILOM Administration > Connectivity > Network > Network Settings**
- User Role: admin (a) (required for all property modifications)

Requirements:

- Standard connectivity configuration properties apply to all servers running Oracle ILOM 3.2.0, 3.2.1, 3.2.2, and 3.2.3. They also apply to some server models running Oracle ILOM firmware 3.2.4 and later. Refer your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made in the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
		■ Both or one of the properties for <code>Autoconfig Stateless</code> and <code>Autoconf DHCPv6_Stateful</code> are enabled in Oracle ILOM. ■ The IPv6 network router or the DHCPv6 server reports multiple dynamic network addresses for the server SP or the CMM. Special Considerations: ■ Oracle ILOM stores up to 10 dynamic addresses in an internal structure. ■ Oracle ILOM responds to all dynamic network addresses. ■ If only the <code>Autoconfig DHCPv6_Stateless</code> property is set, no dynamic network addresses are reported in the Oracle ILOM interfaces. CLI Syntax for Dynamic IPv6 Address: show <code>/SP CMM/network/ipv6</code>
Save Button (<code>commitpending=true</code>)	All pending network modifications	Web interface – All modification made within the Network Settings page must be Saved before they can take affect in Oracle ILOM. CLI – All pending network modifications must be committed under the <code>/network</code> target. Special Considerations: ■ The IPv4 pending modifications take affect after they are committed or saved. ■ Assigning a new static IPv4 address to a managed device will end all active Oracle ILOM sessions to the SP or CMM. To log back in to Oracle ILOM, open a new browser session and enter the newly assigned IPv 4 address. ■ The IPv6 pending modifications take affect after they are committed or saved. Changes to the <code>autoconfig</code> properties do not need to be committed in the CLI. ■ Newly learned auto-configuration IPv6 addresses will not affect any Oracle ILOM session currently connected to the managed device (SP or CMM). CLI Syntax for IPv4 Commit Pending Modification: set <code>/SP CMM/network state=enabled disabled</code> <code>pendingipdiscovery=static dhcp pendingipaddress=value</code> <code>pendingipgateway=value pendingipnetmask=value</code>

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: ILOM Administration > Connectivity > Network > Network Settings
- User Role: admin (a) (required for all property modifications)

Requirements:

- Standard connectivity configuration properties apply to all servers running Oracle ILOM 3.2.0, 3.2.1, 3.2.2, and 3.2.3. They also apply to some server models running Oracle ILOM firmware 3.2.4 and later. Refer your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made in the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
		<code>set /SP CMM/network commitpending=true</code>
		CLI Syntax for IPv6 Commit Pending Modifications:
		<code>set /SP CMM/network/ipv6 state=enabled disabled</code> <code>pending_static_ipaddress=ipv6_address/</code> <code>subnet_mask_length_in_bits</code>
		<code>set /SP CMM/network commitpending=true</code>
		Related Information:
		■ “Test IPv4 and IPv6 Connectivity” on page 145

TABLE 47 Network Connectivity Enhanced Configuration Properties**User Interface Configurable Target and User Role:**

- CLI: `/SP|CMM/network`
- Web: ILOM Administration > Connectivity > Network > Network Settings
- User Role: admin (a) (required for all property modifications)

Requirements:

- The Network Connectivity enhanced configuration settings apply to most new server models and a select number of legacy server models running Oracle ILOM 3.2.4 and later. Refer to your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made to the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
MAC Address	Read-only	<code>macaddress= outofbandaddress= sidebandmacaddress=</code>
Out of Band MAC Address		The media access control (MAC) addresses for the server SP and CMM are set at the factory.
Sideband MAC Address		The MAC Address properties for both the SP and CMM are non-configurable read-only properties in Oracle ILOM.
		CLI Syntax to Show MAC Address Properties:

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: **ILOM Administration > Connectivity > Network > Network Settings**
- User Role: **admin (a)** (required for all property modifications)

Requirements:

- The Network Connectivity enhanced configuration settings apply to most new server models and a select number of legacy server models running Oracle ILOM 3.2.4 and later. Refer to your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made to the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
show /SP CMM/network		
Management Port (managementport=)	MGMT	<i>MGMT NETn</i> All servers shipped with Oracle ILOM include a physical network management port (MGT) used for connecting to Oracle ILOM over a network. Some systems shipped with Oracle ILOM also support sideband management. Sideband management shares the use of a physical data port (NETn) on the server to permit network access to both the host operating system and Oracle ILOM. For systems supporting this option, network administrators can either choose to accept the default Management Port property (MGMT) or modify the Management Port property for sideband management use (NETn). CLI Syntax for SP Management Port: <pre>set /SP/network pendingmanagementport=MGMT NETn</pre> <pre>set /SP CMM/network commitpending=true</pre> Related Information: ■ “Sideband Network Management Connection” on page 20 ■ “Dedicated Network Management Connection (Default)” on page 18
VLAN Tag (pendingvlan_id=)	(none)	<i>Integer between 1 and 4079</i> In Oracle ILOM, VLAN tagging is disabled by default. While VLAN tagging is disabled, the system does not generate VLAN-tagged Ethernet frames and does not process incoming VLAN-tagged Ethernet frames. If you enable VLAN tagging, the system can generate and receive VLAN-tagged Ethernet frames in accordance with the Institute of Electrical and Electronics Engineers (IEEE) 802.1Q standard. Specify the VLAN tag as an integer between 1 and 4079. Alternatively, use a VLAN Tag value of 0 in the web interface or “” in the CLI to disable VLAN tagging. CLI Syntax for VLAN Tag: <pre>set /SP/network pendingvlan_id=[1–4079 “”]</pre> <pre>commitpending=true</pre>
IPv4 State	Enabled	<i>Enabled Disabled</i>

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: ILOM Administration > Connectivity > Network > Network Settings
- User Role: admin (a) (required for all property modifications)

Requirements:

- The Network Connectivity enhanced configuration settings apply to most new server models and a select number of legacy server models running Oracle ILOM 3.2.4 and later. Refer to your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made to the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
(state=)		The IPv4 network State property is enabled by default. Web Property Descriptions for IPv4 State: ■ Enabled (default) — When the Enabled check box for IPv4 State is selected, the Ethernet connection to Oracle ILOM is enabled for IPv4. ■ Disabled — When the Enabled check box for IPv4 State is cleared, the Ethernet connection to Oracle ILOM is disabled for IPv4. CLI Syntax and Property Descriptions for IPv4 State: set <code>/SP CMM/network state=enabled ipv4-only ipv6-only disabled</code> CLI IPv4 Property Descriptions ■ enabled (default) — Set to enabled to operate in a dual-stack IPv4 and IPv6 network environment, where the Ethernet connection to Oracle ILOM is enabled for both IPv4 and IPv6. In this case, the IPv6 State property (<code>/network/ipv6 state=</code>) must also be set to enabled. ■ ipv4-only — When set to <code>ipv4-only</code>, the Ethernet connection to Oracle ILOM is enabled for IPv4 only. ■ ipv6-only — When set to <code>ipv6-only</code>, the Ethernet connection to Oracle ILOM is enabled for IPv6 only. ■ disabled — Set to disabled to prevent both an IPv4 and an IPv6 Ethernet connection to Oracle ILOM.
IPv4 IP Discovery Mode (ipdiscovery=)	DHCP	<i>DHCP Static</i> The property for IPv4 Discovery Mode in Oracle ILOM is set to DHCP by default. When this property is set to DHCP, Oracle ILOM uses DHCP to determine the physical network address for the server SP or CMM. Optionally, network administrators can disable the DHCP property and choose to configure a static IPv4 network address, Netmask address and Gateway address for the server SP or CMM. Note. When DHCP is set, Oracle ILOM uses the default Auto DNS property to assign the DNS named server and search path. For dual-stack DHCP configurations, the DNS settings in Oracle ILOM can be set to receive DNS information from either the IPv4 or the IPv6 DHCP server.

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: **ILOM Administration > Connectivity > Network > Network Settings**
- User Role: admin (a) (required for all property modifications)

Requirements:

- The Network Connectivity enhanced configuration settings apply to most new server models and a select number of legacy server models running Oracle ILOM 3.2.4 and later. Refer to your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made to the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
		Note - Some server SPs, like the SPARC M7 series servers, no longer support the ability to configure an DHCP IP4 address. In this case, the property for IP Discovery displays Static. CLI Syntax for IPv4 IP Discovery Mode: set <code>/SP CMM/network pendingipdiscovery=dhcp static</code> <code>set /SP CMM/network commitpending=true</code> Related Information: ■ Table 48, “DNS Configuration Properties,” on page 134
IPv4	None	<i>None SysID</i>
DHCP Client ID (dhcp_clientid=)		The property for the DHCP Client ID is set to None by default. Optionally, network administrators can set a SysID (System Identifier) for the DHCP Client using the <code>system_identifier</code> property under the <code>/SP</code> target. Note - Some server SPs, like the SPARC M7 series servers, no longer support the ability to configure a DHCP IP4 address. In this case, the property for DHCP Client ID is not available. CLI Syntax for IPv4 DHCP Client ID: show <code>/SP CMM/network dhcp_clientid=none sysid</code> Related Information: ■ “Assigning System Identification Information” on page 140
IPv4 Network Address Netmask Address Gateway Address	Static IP Discovery Mode, Disabled	<code>ipaddress= ipnetmask= ipgateway=</code> Note - IP addresses in the following subnets are reserved and cannot be assigned: 169.254.10.n, 169.254.11.n, 169.254.12.n The IP4 user-configurable address properties for Network, Netmask, and Gateway are disabled in Oracle ILOM by default. Optionally, network administrators can set a Static value for the IP Discovery Mode property and manually populate the static IPv4 addresses for Network, Netmask and Gateway.

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: ILOM Administration > Connectivity > Network > Network Settings
- User Role: admin (a) (required for all property modifications)

Requirements:

- The Network Connectivity enhanced configuration settings apply to most new server models and a select number of legacy server models running Oracle ILOM 3.2.4 and later. Refer to your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made to the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
		Note - Some Oracle server SPs (such as Oracle SPARC M7 series servers) no longer support the ability to configure a DHCP IPv4 address. CLI Syntax for IPv4 Static Addresses: <pre>set /SP CMM/network pendingipaddress=value pendingipnetmask=value pendingipgateway=value</pre> <pre>set /SP CMM/network commitpending=true</pre> Related Information: ■ “Input Format for IPv4 and IPv6 Addresses” on page 98
IPv6 State (/ipv6 state=)	Enabled	<i>Enabled Disabled</i> The IPv6 State property is enabled in Oracle ILOM by default. Optionally, network administrators can disable the IPv6 network state for any network environment that is not dependent on an IPv6 or a dual-stack (IPv4 and IPv6) network connection. When the IPv6 State is set to Enabled, the Oracle ILOM Ethernet network port is enabled for IPv6 network connection. When the IPv6 State is set to Disabled, the Oracle ILOM Ethernet network port is disabled for IPv6 network connections. Note – The properties for IPv4 State and IPv6 State must both be enabled in Oracle ILOM to support a dual-stack (IPv4 and IPv6) network connection. CLI Syntax for IPv6 State: <pre>set /SP CMM/network/ipv6 state=enabled disabled</pre>
IPv6 Autoconfig (/ipv6 autoconfig=)	Stateless	<i>disabled stateless</i> The IPv6 Autoconfig property is set to Stateless in Oracle ILOM by default. When the Autoconfig Stateless property is enabled, Oracle ILOM learns its IPv6 dynamic address prefixes from the IPv6 router. When the IPv6 Autoconfig Stateless property is set to Disabled, the ability for IPv6 Autoconfig is disabled. Special Considerations:

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: **ILOM Administration > Connectivity > Network > Network Settings**
- User Role: admin (a) (required for all property modifications)

Requirements:

- The Network Connectivity enhanced configuration settings apply to most new server models and a select number of legacy server models running Oracle ILOM 3.2.4 and later. Refer to your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made to the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
		■ The IPv6 Autoconfig Stateless options determine the IP address without any IP support from a DHCPv6 server. ■ The IPv6 Autoconfig Stateless property can be enabled in Oracle ILOM regardless of how the property for DHCPv6 Autoconfig is set. CLI Syntax for IPv6 Autoconfig: set <code>/SP CMM/network/ipv6 autoconfig=stateless disabled</code>
DHCPv6 Autoconfig (/ipv6 autoconfig=)	(none)	<i>DHCPv6_Stateless DHCP_Stateful</i> The DHCPv6 Autoconfig property is disabled in Oracle ILOM by default. When this property is disabled, Oracle ILOM is prevented from learning the SP or CMM network addresses and DNS information from a DHCPv6 server on the network. Optionally, network administrators can choose to enable the DHCPv6 Autoconfig property by setting one of the following property values: ■ DHCPv6 Stateless – When enabled, Oracle ILOM automatically learns the DNS information for the server SP (or CMM) from the DHCPv6 network router. ■ DHCPv6 Stateful – When enabled, Oracle ILOM automatically learns the dynamic IPv6 addresses and the DNS information for the server SP (or CMM) from the DHCPv6 network router. Special Considerations: ■ For dual-stack DHCP configurations, the DNS settings in Oracle ILOM can be set to receive DNS information from either the IPv4 or the IPv6 DHCP server. ■ The unique ID for the DHCPv6 server that was last used by Oracle ILOM to retrieve the DHCPv6 network information is identified by the <code>dhcpv6_server_duid</code> property. CLI Syntax for DHCPv6 Autoconfig: set <code>/SP CMM/network/ipv6 autoconfig=dhcpv6_stateless dhcpv6_stateful</code>
Link-Local IPv6 Address (/ipv6 link_local_ipaddress=)	Read-only	The read-only property for Link-Local IPv6 Address is a non-routable address that you can use to connect to the Oracle ILOM SP (or the CMM) from another IPv6-enabled node on the same network.

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: ILOM Administration > Connectivity > Network > Network Settings
- User Role: admin (a) (required for all property modifications)

Requirements:

- The Network Connectivity enhanced configuration settings apply to most new server models and a select number of legacy server models running Oracle ILOM 3.2.4 and later. Refer to your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made to the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
		Oracle ILOM applies the following principles to build the Link-Local Address for the SP or CMM: ■ Oracle ILOM uses the SP or CMM MAC address in conjunction with the link-local identifier prefix. ■ Oracle ILOM, at initialization, uses the Duplicate Address Detection (DAD) protocol to ensure that the reported Local-Link address for the SP (or CMM) is unique. CLI Syntax for Link-Local Address: show <code>/SP CMM/network/ipv6</code>
IPv6 Static IP Address (<code>/ipv6 static_ipaddress=</code>)	None	When the IPv6 state is enabled, network administrators can optionally assign a static IPv6 address to the SP or CMM. Note - IP addresses in the following subnets are reserved and cannot be assigned: 169.254.10.n, 169.254.11.n, 169.254.12.n The parameters for specifying the IPv6 static IP and netmask are: <i>IPv6_address/subnet_mask_length_in_bits</i>. The gateway address, by default, is automatically configured. Example: fec0:a:8:b7:214:4fff:feca:5f7e/64 CLI Syntax for Static IPv6 Address: set <code>/SP CMM/network/ipv6</code> pending_static_ipaddress=ipaddress/subnetmask set <code>/SP CMM/network</code> commitpending=true
IPv6 Static Gateway (<code>/ipv6 static_ipgateway=</code>)	None	You can optionally assign a static IPv6 gateway address that will be used in conjunction with any IPv6 gateway addresses received through router advertisements. IPv6 Static Gateway Example: 2001:db8:0:0:0:379c:a562:bef0 CLI Syntax for IPv6 Gateway: set <code>/SP CMM/network/ipv6</code> pending_static_ipgateway=[user_specified_ipv6_gateway_address]

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: **ILOM Administration > Connectivity > Network > Network Settings**
- User Role: admin (a) (required for all property modifications)

Requirements:

- The Network Connectivity enhanced configuration settings apply to most new server models and a select number of legacy server models running Oracle ILOM 3.2.4 and later. Refer to your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made to the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
set /SP CMM/network commitpending=true		
IPv6 Gateway (/ipv6 ipgateway=)	Read-only	The read-only IPv6 gateway address presented in this property is learned from an IPv6 router on the network. CLI Syntax for IPv6 Gateway: show / SP CMM/network/ipv6
Dynamic IPv6 Address (/ipv6 dynamic_ipaddress_n)	Read-only	Oracle ILOM reports dynamic IPv6 addresses when the following occurs: ■ Both or one of the properties for Autoconfig Stateless and Autoconf DHCPv6_Stateful are enabled in Oracle ILOM. ■ The IPv6 network router or the DHCPv6 server reports multiple dynamic network addresses for the server SP or the CMM. Special Considerations: ■ Oracle ILOM stores up to 10 dynamic addresses in an internal structure. ■ Oracle ILOM responds to all dynamic network addresses. ■ If only the Autoconfig DHCPv6_Stateless property is set, no dynamic network addresses are reported in the Oracle ILOM interfaces. CLI Syntax for Dynamic IPv6 Address: show /SP CMM/network/ipv6
Save Button (commitpending=true)	All pending network modifications	Web interface – All modification made within the Network Settings page must be Saved before they can take affect in Oracle ILOM. CLI – All pending network modifications must be committed under the /network target. Special Considerations: ■ The IPv4 pending modifications take affect after they are committed or saved. ■ Assigning a new static IPv4 address to a managed device will end all active Oracle ILOM sessions to the SP or CMM. To log back in to Oracle ILOM, open a new browser session and enter the newly assigned IPv 4 address.

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/network`
- Web: ILOM Administration > Connectivity > Network > Network Settings
- User Role: admin (a) (required for all property modifications)

Requirements:

- The Network Connectivity enhanced configuration settings apply to most new server models and a select number of legacy server models running Oracle ILOM 3.2.4 and later. Refer to your server administrator guide or product notes to determine which Oracle ILOM IP settings are supported on your system.
- All CLI pending network modifications must be committed to take affect in Oracle ILOM. All web modifications made to the Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
		■ The IPv6 pending modifications take affect after they are committed or saved. Changes to the autoconfig properties do not need to be committed in the CLI. ■ Newly learned auto-configuration IPv6 addresses will not affect any Oracle ILOM session currently connected to the managed device (SP or CMM).
		CLI Syntax for IPv4 Commit Pending Modification: <pre>set /SP CMM/network state=enabled disabled pendingipdiscovery=static dhcp pendingipaddress=value pendingipgateway=value pendingipnetmask=value set /SP CMM/network commitpending=true</pre>
		CLI Syntax for IPv6 Commit Pending Modifications: <pre>set /SP CMM/network/ipv6 state=enabled disabled pending_static_ipaddress= value/ subnet_mask_valuepending_static_ipgatewayaddress= value set /SP CMM/network commitpending=true</pre>
		Related Information: ■ “Test IPv4 and IPv6 Connectivity” on page 145

TABLE 48 DNS Configuration Properties**User Interface Configurable Target and User Role:**

- CLI: `/SP|CMM/clients/dns`
- Web: ILOM Administration > Connectivity > DNS > DNS Configuration
- User Role: admin (a) (required for property modification)

Property	Default Value	Description
Auto DNS via DHCP (auto_dns=)	Enabled	<i>Enabled Disabled</i> The Auto DNS via DHCP property is enabled in Oracle ILOM by default. When this property is enabled, Oracle ILOM automatically retrieves the DNS information from the DHCP server.

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/clients/dns`
- Web: **ILOM Administration > Connectivity > DNS > DNS Configuration**
- User Role: **admin (a)** (required for property modification)

Property	Default Value	Description
		Optionally, network administrators can disable the Auto DNS property to manually configure the DNS information in Oracle ILOM. CLI Syntax for Auto DNS via DHCP: set <code>/SP CMM/clients/dns auto_dns=enabled disabled</code>
DNS Named Server (nameserver=)	None	When the Auto DNS property is disabled, up to three IP addresses are manually configurable in the DNS Named server property. When entering multiple IP addresses, follow these guidelines: ■ Each address must be separated by a comma. ■ When mixing IPv4 and IPv6 addresses, list the IPv4 address(es) first. CLI Syntax for DNS Named Server: set <code>/SP CMM/clients/dns nameserver=ip_address_1, ipaddress_2, ipaddress_3</code>
DNS Search Path (searchpath=)	None	When the Auto DNS property is disabled, up to six domain suffixes are manually configurable in the DNS Search Path property. Each search suffix must be separated by a comma. CLI Syntax for DNS Search Path: set <code>/SP CMM/clients/dns searchpath= domain_1.com, domain_2.edu, and so on</code>
DNS Timeout (timeout=)	5 seconds	Integer between 1 and 10 The DNS Timeout property value specifies how many seconds the DNS server is allotted to complete a DNS query. Optionally, network administrators can increase or decrease the default timeout value allotted to the DNS server. DNS Timeout CLI Syntax: set <code>/SP CMM/clients/dns timeout=n</code> Related Topic: ■ “Example Setup of Dynamic DNS” on page 137
DNS Retries (retries=)	1 retry	Integer between 0 and 4 The DNS Retries property value specify how many times a DNS query is retried in the event of a timeout.

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/clients/dns`
- Web: ILOM Administration > Connectivity > DNS > DNS Configuration
- User Role: admin (a) (required for property modification)

Property	Default Value	Description
		Optionally, network administrators can increase or decrease the default DNS Retries property value. DNS Retries CLI Syntax: set /SP CMM/clients/dns retries=<i>n</i>
Save Button (web only)		Web interface – Changes made within the DNS Configuration page must be saved in Oracle ILOM before they can take affect.

TABLE 49 Serial Port Configuration Properties**User Interface Configurable Target:**

- CLI: `/SP/serial/portsharing`
- Web: ILOM Administration > Connectivity > Serial Port > Serial Port Settings
- User Role: (a) Admin (required for property modification)

Property	Default Value	Description
Owner (owner=)	SP	<i>SP hostserver</i> The serial port Owner property is configurable on some Oracle servers. For further information, see “Serial Management Port Owner” on page 98 . CLI Syntax for Serial Port Owner: set /SP/serial/portsharing owner=SP hostserver
Host Serial Port (/host pendingspeed= flowcontrol=)	Baud Rate= 9600 Flow Control= None	Baud Rate = 9600 Flow Control = <i>Software Hardware None</i> The Host Serial Port properties are configurable on some Oracle servers. The property values for the Host Serial Port option must match the property values set for the serial console port on the host server. Often referred to as serial port 0, COM1, or /dev/ttyS0. CLI Syntax for Host Serial Port: set /SP CMM/serial/host pendingspeed=<i>value</i> flowcontrol=<i>value</i> commitpending=true
External Serial Port (/external pendingspeed= flowcontrol=)	Baud Rate= 9600 Flow Control= None	Baud Rate = 9600 Flow Control = <i>None</i> The external serial port on a managed device is the serial management (SER MGT) port. Optionally, network administrators can change the default baud rate speed for the external serial port. CLI Syntax for External Serial Port:

User Interface Configurable Target:

- CLI: /SP/serial/portsharing
- Web: ILOM Administration > Connectivity > Serial Port > Serial Port Settings
- User Role: (a) Admin (required for property modification)

Property	Default Value	Description
		set /SP CMM/serial/external pendingspeed=value commitpending=true
Save Button (web only)		Web interface – Changes made within the Serial Port Settings page must be saved in Oracle ILOM before they can take affect.

Example Setup of Dynamic DNS

By setting up a Dynamic Domain Name Service (DDNS), you can further leverage DHCP to automatically make the DNS server in your network environment aware of the host names for all newly added Oracle ILOM systems using DHCP.

When DDNS is configured, network administrators can determine the host name of a specific Oracle ILOM SP or CMM by combining the product serial number with one of these prefixes: SUNSP or SUNCMMn. For example, given a product serial number of 0641AMA007, the host name for a server SP would be SUNSP-0641AMA007, the host name for a single chassis-installed CMM would be SUNCMM-0641AMA007, and the host names for two chassis-installed CMMs would be SUNCMM0-0641AMA007 and SUNCMM1-0641AMA007.

▼ Example: Set Up DDNS Configuration

This example describes how to set up a typical DDNS configuration.

Assumptions:

The following assumptions apply to this DDNS configuration example:

- There is a single server that handles both DNS and DHCP for the network on which the SP resides.
- The SP network address is 192.168.1.0.
- The DHCP/DNS server address is 192.168.1.2
- The IP addresses from 192.168.1.100 to 192.168.1.199 are used as a pool to provide addresses to the SP and other clients.
- The domain name is example.com.

- There is no existing DNS or DHCP configuration in place. If there is, use the `.conf` files in this example as a guideline to update the existing configuration.

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

You can use the following steps and sample files provided here, with site-specific modifications, to set up your own DDNS configuration.

1. **Install the `bind9` and `dhcp3-server` packages from the Debian distribution.**
Installing the `dnsutils` package provides access to `dig`, `nslookup`, and other useful tools.
2. **Using `dnssec-keygen`, generate a key to be shared between the DHCP and DNS servers to control access to the DNS data.**
3. **Create a DNS configuration file named `/etc/bind/named.conf` that contains the following:**

```
options {
    directory "/var/cache/bind";
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/etc/bind/db.root";
};
// be authoritative for the localhost forward and reverse zones, // and for broadcast
zones as per RFC 1912
zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};
```

```

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
// additions to named.conf to support DDNS updates from dhcp server
key server.example.com {
    algorithm HMAC-MD5;
    secret "your-key-from-step-2-here"
};
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
    allow-update { key server.example.com; };
};
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.example.rev";
    allow-update { key server.example.com; };
};

```

4. Add empty zone files for the local network.

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

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

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

```

ddns-update-style interim;
ddns-updates      on;
server-identifier server;
ddns-domainname   "example.com.";
ignore client-updates;
key server.example.com {
    algorithm hmac-md5;
    secret your-key-from-step-2-here;
}
zone example.com. {
    primary 127.0.0.1;
    key server.example.com;
}
zone 1.168.192.in-addr.arpa. {
    primary 127.0.0.1;
    key server.example.com;
}
default-lease-time 600;

```

```

max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.199;
    option domain-name-servers 192.168.1.2;
}

```

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

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

References

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

Assigning System Identification Information

Oracle ILOM provides a set of configurable properties to help identify a specific managed device in your environment. System administrators can use these parameters to uniquely identify the physical location of a managed device, the point-of-contact of a managed device, and the host name assigned to a managed device. For further system identification configuration details, see the following tables.

TABLE 50 Device Identification Configuration Properties

User Interface Configurable Target and User Role:		
■ CLI: <code>/SP/</code> ■ Web: ILOM Administration > Identification ■ User Role: Admin (a) (required for property modification)		
Property	Default Value	Description
Host Name (hostname=)	Oracle branding string	The default Host Name is formed by concatenating an Oracle branding string, such as "ORACLESP-" or "ORACLECOMM-", with the system-level serial number. The Host Name can contain up to 60 characters in length. It must begin with a letter and contain only alphanumeric, hyphen, and underscore characters. Note - As of Oracle ILOM 4.0.4, the system-level serial number max size was increased to 64 bytes. As a result, the HOST Name will be truncated when the length of the serial number field is over 50 bytes. In this case, the system administrator should overwrite the default Host Name with a customer defined Host Name.
CLI Syntax for Host Name:		

User Interface Configurable Target and User Role:

- CLI: /SP/
- Web: ILOM Administration > Identification
- User Role: Admin (a) (required for property modification)

Property	Default Value	Description
		set /SP CMM hostname=value
System Identifier (/system_identifier=)	None	The System Identifier, when defined, helps identify the managed device in the payload element of an SNMP trap. The System Identifier property value can contain up to 60 characters using any standard keyboard keys except quotation marks. This property is configurable in both the server SP and CMM. CLI Syntax for System Identifier: set /SP CMM system_identifier=value
System Contact (/system_contact=)	None	The System Contact, when defined, helps identify the point-of-contact for the managed device such as the name or email address of the person responsible for the device. The System Contact property value can consist of a text string using any standard keyboard keys except quotation marks. CLI Syntax for System Contact: set /SP CMM system_contact=value
System Location (/system_location=)	None	The System Location, when defined, helps identify the physical location of a managed device such as a rack identifier or a data center location. The system location property value can consist of a text string using any standard keyboard keys except quotation marks. CLI Syntax for System Location: set /SP CMM system_location=value
Physical Presence Check (/check_physical_presence=)	Enabled	The Physical Presence Check affects the behavior for recovering the preconfigured Oracle ILOM root account password. ■ Enabled (true) – When enabled, the Locator button on the physical system must be pressed in order to recover the default Oracle ILOM password. Note - On some Oracle servers, the physical presence is indicated by a different method than the Locator button. ■ Disabled (false) – When disabled, the default Oracle ILOM administrator password can be reset without pressing the Locator button on the physical system. CLI Syntax for Physical Presence Check: set /SP CMM check_physical_presence=true false Related Topic:

User Interface Configurable Target and User Role:

- CLI: /SP/
- Web: ILOM Administration > Identification
- User Role: Admin (a) (required for property modification)

Property	Default Value	Description
		■ Table 13, “Recover Preconfigured root Account or root Account Password (CLI only),” on page 49
Save Button (web only)		Web interface – Changes made within the Identification page must be saved in Oracle ILOM before they can take affect.

Setting ILOM Clock Properties

When deploying Oracle ILOM for the first time, system administrators should configure the clock settings in Oracle ILOM to ensure that the system management events logged by Oracle ILOM appear with the correct timestamps.

System administrators can choose to either synchronize the Oracle ILOM clock with an NTP server or manually configure the date and time locally in Oracle ILOM using the UTC/GMT timezone on the host server.

For Oracle ILOM clock configuration properties, see the following table.

TABLE 51 Oracle ILOM Clock Configuration Properties

User Interface Configurable Target and User Role:		
■ CLI: /SP CMM/clock ■ Web: ILOM Administration > Date and Time > Clock Settings Timezones ■ User Role: admin (a) (required for property modification)		
Property	Default Value	Description
Date and Time (datetime=)	None	Populate the Date property with the month, day, and year. Populate the Time property with the hours and minutes. CLI Syntax to Set Date and Time: set /SP CMM/clock datetime=MMDDhhmmYYYY
Timezones (timezones=)	None	Timezone Abbreviations (PST, EST, and so on) Populate the Timezones property with the appropriate timezone. CLI Syntax to Set Timezones: set /SP CMM/clock timezones=3_to_4_characters
Synchronize Time with NTP Server	Disabled	<i>Enabled Disabled</i>

User Interface Configurable Target and User Role:

- CLI: `/SP|CMM/clock`
- Web: ILOM Administration > Date and Time > Clock Settings | Timezones
- User Role: admin (a) (required for property modification)

Property	Default Value	Description
(usntpserver=)		When set to disabled, the Oracle ILOM clock will not synchronize with an NTP server. When set to enabled, the Oracle ILOM clock will synchronize with the designated Network Time Protocol (NTP) server. Note - When enabled, you can set the Oracle ILOM clock to synchronize with one or two Network Time Protocol (NTP) servers. CLI Syntax to Synchronize Clock With NTP Server: set <code>/SP CMM/clock usntpserver=enabled disabled</code>
NTP Server 1 (2) (<code>/SP CMM/clients/ntp/server/n address=<address></code>)	None	Set the IP address or DNS host name of the NTP server or servers with which the Oracle ILOM clock will synchronize. Configuring two NTP servers provides redundancy. CLI Syntax to Set NTP Server Address: set <code>/SP CMM/clients/ntp/server/1 address=<address></code> set <code>/SP CMM/clients/ntp/server/2 address=<address></code> Note - Some managed devices support the configuration of more than two NTP servers.
Save Button (web only)		Web interface – Changes made within the Clock Settings page and the Timezone Settings page must be saved in Oracle ILOM before they can take affect.

Refer to the Oracle server documentation to determine whether:

- The current time in Oracle ILOM can persist across SP reboots.
- The current time in Oracle ILOM can be synchronized with the host at host boot time.
- The system supports a real-time clock element that stores the time.

Suggested Resolutions for Network Connectivity Issues

- [“Resolving Connectivity Issues” on page 144](#)
- [“Recommended Practice for Spanning Tree Configurations ” on page 145](#)
- [“Test IPv4 and IPv6 Connectivity” on page 145](#)

Resolving Connectivity Issues

If you are experiencing difficulties establishing a network connection to Oracle ILOM interfaces, refer to the following IPv4 and IPv6 information for suggested resolutions.

- [Table 52, “Troubleshooting IPv4 Connectivity Issues,” on page 144](#)
- [Table 53, “Troubleshooting IPv6 Connectivity Issues,” on page 144](#)

TABLE 52 Troubleshooting IPv4 Connectivity Issues

Problem	Suggested Resolution
Unable to access Oracle ILOM using IPv4 from a network client.	Ensure that the setting for State is enabled on the Network Settings page in the Oracle ILOM web interface or under the <code>/SP/network</code> target in the Oracle ILOM CLI. Other suggestions for diagnosing IPv4 network issues, include the following: ■ Verify that a LAN connection to the physical management port (NET MGT) is established. ■ Verify that the appropriate network service, in Oracle ILOM, is enabled: 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 or the CLI. Or, run traceroute from the service Oracle ILOM restricted shell.

TABLE 53 Troubleshooting IPv6 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>
Unable to access Oracle ILOM using IPv6 from a network client.	If on a separate subnet, try the following: ■ Verify that Oracle ILOM has a dynamic or static address (not just a Link-Local address). ■ Verify that the network client has an IPv6 address configured (not just a Link-Local address). If on the same or a separate subnet, try the following: ■ Ensure that the property for IPv6 State 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, in Oracle ILOM, is enabled: 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 IPv6 Ping or Traceroute to test the network connection to the managed device.

Problem	Suggested Resolution
	Run <code>ping6</code> from the web or CLI. Or, run <code>tracert</code> from the service Oracle ILOM restricted shell.

Recommended Practice for Spanning Tree Configurations

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

When configuring Spanning Tree parameters, consider these recommendations:

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

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

▼ Test IPv4 and IPv6 Connectivity

To send a network test from the IP and gateway addresses configured in Oracle ILOM to a device on the network, follow this procedure:

● Perform one of the following:

■ CLI:

To issue a ping connectivity test from the CLI, type one of the following:

```
set /SP|CMM/network/test ping=device_ip4_address_on_network
```

```
set /SP|CMM/network/test ping6=device_ip6_address_on_network
```

If the test failed, an error message appears. On some Oracle servers a succeed message appears if the test succeeded.

- **Web:**

To issue a ping connectivity test from the web, do the following:

- a. **Click ILOM Administration > Connectivity > Network > Network Tools.**
- b. **In the tools dialog, select a test type, specify an IP address of a device on the network, then click Test.**

Related Information:

- [Table 46, “Network Connectivity Standard Configuration Properties ,” on page 119](#)

Using Remote KVMS Consoles for Host Server Redirection

Description	Links
Refer to this section to determine the host server redirection KVMS console options supported on Oracle's Sun systems.	■ “Oracle ILOM Remote KVMS Consoles Supported” on page 148
Refer to this section for instructions for establishing a serial redirection session to the host server from the Oracle ILOM CLI.	■ “Establishing a Host Serial Console Session to the Server (CLI)” on page 149
Redirect a storage image file from a remote NFS or SAMBA server to the host server.	■ “Redirecting an Image File From a Storage Device to the Host Server” on page 155
For SPARC M7 or T7 Series Servers, manage the preinstalled Solaris Miniroot package.	■ “Uploading a New Solaris Miniroot Package From SP to Host ” on page 160
Redirect the remote server keyboard, video, and mouse by launching a VNC viewer from your desktop to the Solaris host VNC server.	■ “Connecting to the Oracle ILOM Remote System VNC Console” on page 163

Related Information

- [“Using the Oracle ILOM Remote System Console or Storage Redirection CLI” on page 167](#)
- [“Using the Oracle ILOM Remote System Console Plus” on page 197](#)
- [“Using Remote KVMS Securely” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x](#)

Oracle ILOM Remote KVMS Consoles Supported

To determine the remote KVMS capabilities supported on a managed device, see the following table:

KVMS Console	Description	Firmware Versions	Managed Device	More Details
Oracle ILOM Remote System Console Storage Redirection CLI	The Oracle ILOM Remote System Console enables you to remotely redirect the host server keyboard, video, mouse and storage (KVMS) events to a graphical shared desktop display. Using the SP or CMM web interface, you can deploy serial or video redirection client sessions over the configured management network to the host server. The Storage Redirection CLI client service enables you to redirect remote storage devices on a host server to a command-line shell display.	Managed devices that upgraded from firmware version 3.1.x to 3.2.x or from firmware version 3.1.x to 3.2.1 or later.	■ Legacy x86 servers ■ Legacy SPARC servers ■ CMM for blade server management	“Using the Oracle ILOM Remote System Console or Storage Redirection CLI” on page 167.
Oracle ILOM Remote System Console Plus	The Oracle ILOM Remote System Console Plus enables you to remotely redirect the host server keyboard, video, mouse, and storage (KVMS) events to a graphical shared desktop display. Using the SP or CMM web interface, you can deploy serial or video redirection client sessions over the configured management network to the host server.	Managed devices shipping with firmware version 3.2.1.x and later.	■ x86 servers ■ SPARC servers (T7, M7, and T8). Note: Remote Console Plus is not supported on M8 series servers as of firmware release 4.0.1.x. ■ CMM for blade server management Note - S7-2 SPARC servers support serial redirection mode only.	“Using the Oracle ILOM Remote System Console Plus” on page 197.
Oracle ILOM Remote System VNC Console	The Oracle ILOM Remote System VNC Console is an implementation of the Virtual Network Computing (VNC) system. It enables you to remotely redirect the host server keyboard, video, and mouse (KVM) events to a graphical shared desktop display.	SPARC servers shipping with firmware version 3.2.6.x and later.	■ SPARC S7-2, T7, M7, and next generation SPARC series servers.	“Connecting to the Oracle ILOM Remote System VNC Console” on page 163

KVMS Console	Description	Firmware Versions	Managed Device	More Details
	Using the SP address and a VNC viewer from your desktop, you can directly deploy a VNC client session over the internal Local Host Interconnect (LANoverUSB) management interface to the Solaris host VNC server.			
Host Storage Redirection	The Host Storage Redirection feature in Oracle ILOM, enables you to redirect a storage image file from a central NFS, SAMBA, or SSHFS repository to the host server. Note - As of Oracle ILOM firmware version 3.2.5.5 and later, a Mini-root mode is supported on newer SPARC servers (T7, M7, and later series servers) for viewing or recovering a Solaris image.	Managed devices shipping with 3.2.1.x and later. Support for the SSHFS redirection option is supported in Oracle ILOM as of firmware version 4.0.3.	■ x86 servers ■ SPARC servers.	“Redirecting an Image File From a Storage Device to the Host Server” on page 155
Host Serial Console (CLI)	Using the SP CLI, you can deploy a serial-based console session over the configured management network to the remote host server.	Managed devices shipping with firmware version 3.0.x and later.	All Oracle servers	“Establishing a Host Serial Console Session to the Server (CLI)” on page 149

Establishing a Host Serial Console Session to the Server (CLI)

System administrators can start or stop a host serial redirection console session from the Oracle ILOM CLI. For further instructions for starting and stopping a host serial console session from the CLI, see the following:

- [“Start Serial Console Redirection and Log In to Host Server OS” on page 149](#)
- [“Dump Full Console History Contents to Remote Location” on page 151](#)
- [“Host Serial Console Log Properties” on page 152](#)

▼ Start Serial Console Redirection and Log In to Host Server OS

Before You Begin

- Console (c) role is required in Oracle ILOM to launch a serial redirection session to the host server operating system.

Note - For Oracle's Sun servers supporting the Oracle ILOM Remote System Console Plus client, the read-write and view-only modes in an Oracle ILOM CLI host console (HOST/console) session are determined by the serial-line redirection setting in the Oracle ILOM Remote System Console Plus client window. For instance, when full-control mode is enabled for serial-line redirection in the Oracle ILOM Remote System Console Plus client window, all active CLI host console sessions will be forced to view-only mode. To regain read-write mode in the CLI host console session, the primary KVM user must relinquish full-control in the Oracle ILOM Remote System Console Plus client window, and then restart session (by typing `start -f /HOST/console`).

- Review [“Host Serial Console Log Properties” on page 152](#). Also, for SPARC multi-domain servers, see [Table 55, “Host Status History Log for SPARC PDomains,” on page 155](#).
- Host server user credentials are required to access the host operating system. Users should log out of the host operating system prior to terminating the host redirection session from Oracle ILOM.
- Host console serial redirection sessions can be started from an Oracle ILOM SP CLI, or by using the serial redirection mode available in the Oracle ILOM Remote System Console Plus.

Note - Solaris users must use serial-redirection to access the Solaris Host Console, view Solaris Host Console messages, or to issue Solaris Host Console commands such as boot commands. Video redirection must not be used to access the Solaris Host Console, view Solaris Host Console messages, or to issue Solaris Host Console commands such as boot commands.

1. To start a host serial redirection console from the Oracle ILOM SP CLI, perform one of the following:

- For single host server SP, type:
`start /host/console`
- For multi-domain SPARC server SP, type:
`start /Servers/PDomains/PDomain_n/host/console`

A message appears prompting you to specify user credentials.

2. **Type the required user credentials to access the host server operating system.**

You are now logged in to the host server operating system through the host serial console.

Note - To issue standard Oracle ILOM CLI commands, you must first exit the host serial console.

3. **To terminate the host redirection session, perform the following:**

- a. **Log out of the host server operating system.**
- b. **To terminate the connection between the host serial console and Oracle ILOM do one of the following:**
 - **For x86 systems, press these keys together: Esc and (**
 - **For SPARC systems, type #.**

Note - To send a break to the host, press the Escape key and type uppercase B.

▼ **Dump Full Console History Contents to Remote Location**

As of Oracle ILOM firmware version 4.0.2, system administrators can use the dump command to transfer the logged history contents of a host serial console session to a specified remote location, such as a remote host or a URI repository. For further instructions, follow these steps:

Note - The Dump Console History feature is not supported on multi-domain platforms, such as the SPARC M-Series servers.

1. **Perform one of the following:**

■ **Dump Full Console History to a Remote Host:**

1. In the Oracle ILOM CLI , type:

```
set /HOST/console  
dump_uri=file_transfer_method://user_name:password@IP_address/file_path/filename
```

For example:

```
set /HOST/console dump_uri=sftp://ilom:changeme@169.254.182.7/tmp/consfile_1031
```

■ Dump Full Console History to a Remote URI Respository:

In the Oracle ILOM CLI , type:

```
dump /HOST/console -destination
file_transfer_method://username:password@IP_address/file_path/filename
```

For example:

```
dump /HOST/console -destination sftp://ilom:changeme@169.254.182.7/tmp/consfile_1031
```

For further information about using the /Host/console dump command, type: **help /host/console dump**

Note - Supported *file_transfers_methods* include: tftp, ftp, sftp, http, or https

2. Upon the successful completion of the /Host/console dump operation, the message **Dump Successful** appears. If the dump operation fails, an error message appears identifying the cause for the error.

Host Serial Console Log Properties

Oracle ILOM provides a set of properties that enables system administrators to configure 1) how the host serial console history log appears, and 2) which escape characters are used to terminate the host serial console redirection session. For descriptions of these properties, see the following tables ([Table 54, “Host Serial Console Log Properties,” on page 152](#) or [Table 55, “Host Status History Log for SPARC PDomains ,” on page 155](#))

Note - CLI paths for multi-domain servers are not specified in the following Host Serial Console Log Properties table. For these type of SPARC servers, append /Servers/PDomains/PDomain_n to the start of the CLI paths described in the following table.

TABLE 54 Host Serial Console Log Properties

User Interface Configurable Target and User Role:		
■ SP CLI: /HOST/console (or, /Servers/PDomain/PDomain_n/Host/console) ■ User Role: - Admin (a) role is required to modify the logging and escapechars properties. - Console (c) role is required to modify the line_count, pause_count, and start_from properties.		
Property	Default	Description
logging	enabled	enabled disabled

User Interface Configurable Target and User Role:

- SP CLI: `/HOST/console` (or, `/Servers/PDomain/PDomain_n/Host/console`)
- User Role:
 - Admin (a) role is required to modify the `logging` and `escapechars` properties.
 - Console (c) role is required to modify the `line_count`, `pause_count`, and `start_from` properties.

Property	Default	Description
		Set the logging property to turn on or turn off serial console history logging. If the logging property is set to disabled, the <code>show /HOST/console/history</code> command will return the following error: <pre>failed. could not get console history</pre> CLI Syntax for logging: Single host server: <pre>set /HOST/console logging=enabled disabled</pre> Multi-domain host server: <pre>set /Servers/PDomain/PDomain_n/HOST/console logging=enabled disabled</pre>
<code>line_count</code>	0	Integer between 0 and 2048 Specify how many lines of the serial console history log to display. A value of 0 instructs Oracle ILOM to display the entire history log. CLI Syntax for line_count: Single host server: <pre>set /HOST/console line_count=0 to 2048</pre> Multi-domain host server: <pre>set /Servers/PDomains/PDomain_n/HOST/console line_count=0 to 2048</pre>
<code>pause_count</code>	0	Integer between 0 and 2048 Specify how many lines of the serial console history log to display at once. After the specified number of lines have been displayed, Oracle ILOM will prompt you to continue: <pre>press any key to continue or ???q' to quit</pre> A value of 0 instructs Oracle ILOM to display the entire history log at once. CLI Syntax for pause_count: <pre>set /HOST/console pause_count=0 to 2048</pre>
<code>start_from</code>	end	<i>beginning end</i>

User Interface Configurable Target and User Role:

- SP CLI: `/HOST/console` (or, `/Servers/PDomain/PDomain_n/Host/console`)
- User Role:
 Admin (a) role is required to modify the logging and escapechars properties.
 Console (c) role is required to modify the line_count, pause_count, and start_from properties.

Property	Default	Description
		Set the start_from property to instruct Oracle ILOM whether to display the serial console history log from the beginning or from the end. CLI Syntax for start_from: Single host server: set /HOST/console start_from=beginning end Multi-domain host server: set /Servers/PDomains/PDomain_n/HOST/console start_from=beginning end
escapechars	#.	Specify the escape characters used to exit the console redirection session. CLI Syntax for escapechars: Single host server: set /HOST/console escapechars=characters Multi-domain host server: set /Servers/PDomains/PDomain_n/HOST/console escapechars=characters Note - The escapechars property is only available for SPARC systems.
timestamp	no (display is disabled)	no (default) yes To display timestamp entries in the console history log from an x86 server SP, set the timestamp property to yes. CLI Syntax for timestamp: set /HOST/console escapechars=yes no Note - The timestamp property is only available on x86 servers as of firmware release 3.2.5 or later.
history	N/A	View host console log history. CLI Syntax for history: Single server: show /HOST/console/history

User Interface Configurable Target and User Role:

- SP CLI: /HOST/console (or, /Servers/PDomain/PDomain_n/Host/console)
- User Role:
Admin (a) role is required to modify the logging and escapechars properties.
Console (c) role is required to modify the line_count, pause_count, and start_from properties.

Property	Default	Description
		Multi-domain server:
		show /Servers/PDomains/PDomain_n/HOST/console/history

TABLE 55 Host Status History Log for SPARC PDomains**User Interface Configurable Target:**

- SP CLI: /Servers/PDomains/PDomain_0/HOST/status_history
 - Web: Host Management >Status History Log
- Status History Log available as of ILOM 3.2.5 firmware release for SPARC multi-domain servers.

Property	Default	Description
list	N/A	View host status history log for SPARC multi-domain servers.
		Web: Click the More details... link on the Status History page for a description of the status log history.
		CLI Syntax to View Host Status History List:
		show /Servers/PDomains/PDomain_0/HOST/status_history/ list

Redirecting an Image File From a Storage Device to the Host Server

Use Host Storage Device feature in Oracle ILOM to either: 1) mount a storage image from an NFS, SAMBA, or SSHFS server and redirect it as an attached host storage device or, 2) configure the service processor (SP) to make the Oracle Solaris Miniroot package that is installed on the SP available to the host on the managed server.

Note - The Host Storage Device Miniroot mode is available only on SPARC M7, T7, and T8 series servers.

Note - The SSHFS file redirection option is available for configuration as of Oracle ILOM 4.0.3.

An NFS, SAMBA, or SSHFS redirection configuration is helpful when you want to boot your server from a single file that is currently stored on a remote NFS, SAMBA, or SSHFS server. A Miniroot redirection configuration is useful for when you want to restore the Oracle Solaris Miniroot package from the Oracle ILOM SP.

For further details about configuring the host storage device properties in Oracle ILOM, see the following information:

- [“Special Considerations for Configuring Host Storage Device Properties” on page 156](#)
- [“CLI and Web Host Storage Device Properties” on page 157](#)
- [“Uploading a New Solaris Miniroot Package From SP to Host ” on page 160](#)

Special Considerations for Configuring Host Storage Device Properties

- The Oracle ILOM Host Storage Device feature is available only on systems that support the Oracle ILOM Remote System Console Plus.

Note - SPARC M8 series servers, as of firmware release 4.0.1.x, do not support Oracle ILOM Remote System Console Plus. SPARC M8 series servers support Oracle ILOM Remote System VNC Console. For further details, see [“Connecting to the Oracle ILOM Remote System VNC Console” on page 163](#)

- Only one storage image can be redirected at one time from any Oracle ILOM KVMS user interface. For instance, if you attempt to redirect a storage image file when another KVMS storage redirection is in progress, the subsequent storage redirection attempt will fail and an error message will appear.
- The Host Storage Device Miniroot mode is available in Oracle ILOM as firmware release 3.2.5.5 for SPARC M7, T7, and later series servers.
- Prior to Oracle ILOM release 3.2.4, the Host Storage Device feature was known as the Remote Device feature (accessible from the web interface by clicking Remote Control -> Remote Device).
- For SPARC server configurations with multiple hosts (domains), you must precede the SP CLI target shown in the Host Storage Device Properties table below with `/Servers/PDomains/PDomain_n`. Navigation in the web interface is as follows: Domain# > Remote Control > Host Storage Device.

CLI and Web Host Storage Device Properties

User Interface Configurable Target and User Role:

- **SP CLI:** `/SP/services/kvms/remote_virtual_device`
- **Web:** Remote Control > Host Storage Device
- **User Role:** Admin (a) role is required to configure the Remote Device properties. Read-Only (o) role is required to view the current settings.

Property	Default	Description
mode	disabled (for systems using SP firmware 3.2.4 or earlier)	<i>disabled remote miniroot</i>
(mode)	miniroot (for newer SPARC M7 and T7 series servers with Solaris OS image preinstalled and using SP firmware 3.2.5.5 or later)	The Mode property controls the Host Storage Device redirection behavior. ■ Disabled — Select Disabled to deactivate the host storage redirection service in Oracle ILOM ■ Remote — Select Remote to redirect a virtual storage image mounted on a remote NFS, SAMBA, or SSHFS server as an attached host storage device. ■ Miniroot — Select Miniroot to configure the SP to point to the pre-loaded Solaris Miniroot package that is currently installed on the managed server. For instructions on how to upload a new Solaris Miniroot package to managed server from SP, see “Uploading a New Solaris Miniroot Package From SP to Host ” on page 160. Note - The Miniroot option is available only on SPARC T7, M7, or later SPARC series servers.

CLI Syntax for mode:

Single server:

```
set /SP/services/kvms/host_storage_device
mode=[disabled|remote|miniroot]
```

Note - The Miniroot option is available on SPARC T7 and M7 servers only.

Multi-domain server:

```
set /Servers/PDomains/PDomains-n/SP/services/kvms/
host_storage_device mode=[disabled|remote| miniroot]
```

Server URI	(none)	<i>NFS, Samba, or SSHFS URI</i>
(target_URI)		Note - As Oracle ILOM firmware version 4.0.3, the SSHFS server URI option is available for configuration. This option supports user authentication through the use of a username and password or a user generated SSH key. To use SSH key-based authentication, copy the public key for the authentication type used (either DSA or RSA) from <code>/SP/services/ssh/keys/rsa dsa</code> to the account for username and put it in the <code>.ssh/authorized_keys</code> file. For additional information about generating a public SSH key for user authentication, see, “CLI Authentication Using Local User SSH Key ” on page 48.

User Interface Configurable Target and User Role:

- **SP CLI:** `/SP/services/kvms/remote_virtual_device`
- **Web:** Remote Control > Host Storage Device
- **User Role:** Admin (a) role is required to configure the Remote Device properties. Read-Only (o) role is required to view the current settings.

Property	Default	Description
		Note - The SAMBA option supports user authentication through the use of username and password. When the Host Storage Device Mode is set to Remote, enter the location of the image on the remote server using either the NFS, Samba, or SSHFS protocol. ■ To enter a URI using NFS, use the following format: <code>nfs://server:/path/file</code> Sample NFS URI: <code>nfs://198.51.100.2:/export/robert/biosimage.img</code> ■ To enter a URI using Samba, use the following format: <code>smb://server:/path/file</code> or <code>smb://server/path/file</code> Sample Samba URI: <code>smb://198.51.100.2/robert/biosimage.img</code> ■ To enter a URI using SSHFS, use the following format: <code>sshfs://host:/file_path</code> Sample SSFS URI: <code>sshfs://198.51.100.100:/export/john/example.img</code> CLI Syntax for target_URI: Single server: <pre>set /SP/services/kvms/host_storage_device target_URI=NFS_or_Samba_or_SSHFS_URI</pre> Multi-domain server: <pre>set /Servers/PDomains/PDomain_n/SP/ services/kvms/host_storage_device target_URI=NFS_or_Samba_or_SSHFS_URI</pre>
Remote Storage User Name (username)	(none)	<i>SAMBA Server username or SSHFS Server user name</i> If you are mounting the virtual storage device using a SAMBA or SSHFS server URI, authentication is required. When Host Storage Device mode is set to Remote, do the following: ■ For SAMBA URI redirection, enter SAMBA Server user name. ■ For SSHFS URI redirection, enter your SSHFS Server user name. CLI Syntax for username: Single server:

User Interface Configurable Target and User Role:

- SP CLI: `/SP/services/kvms/remote_virtual_device`
- Web: Remote Control > Host Storage Device
- User Role: Admin (a) role is required to configure the Remote Device properties. Read-Only (o) role is required to view the current settings.

Property	Default	Description
		set /SP/services/kvms/host_storage_device username=username Multi-domain server: set /Servers/PDomains/PDomain_n/SP/services/kvms/host_storage_device username=username
Remote Storage Password (password)	(none)	<i>SAMBA Server password or SSHFS Server password</i> If you are mounting the virtual storage device using Samba, authentication is required. When Host Storage Device mode is set to Remote, do the following: ■ For SAMBA URI redirection, enter your SAMBA Server password. ■ For SSHFS URI redirection, enter your SSHFS Server password when not using SSH keys for authentication. CLI Syntax for password: Single server: set /SP/services/kvms/host_storage_device password=password Multi-domain server: set /Servers/PDomains/PDomain_n /SP/services/kvms/host_storage_device password=password
Status (status)	disabled	The read-only Status property indicates the operational state of the Remote Device redirection service. The possible values of the Status property are as follows: ■ Connecting – Indicates that the transfer to the host over USB has terminated or has not been established ■ Device not mounted – The virtual storage device image was not mounted successfully. ■ Disabled – The Service State property for Remote Device redirection is set to disabled. ■ Internal file error – A problem occurred in Oracle ILOM when attempting to mount the device. ■ Operational – The virtual storage device redirection has been started successfully.

User Interface Configurable Target and User Role:

- **SP CLI:** /SP/services/kvms/remote_virtual_device
- **Web:** Remote Control > Host Storage Device
- **User Role:** Admin (a) role is required to configure the Remote Device properties. Read-Only (o) role is required to view the current settings.

Property	Default	Description
		■ Remote file transfer error – There was an error when transferring data for the remote device. ■ Remote file configured in URI not found – The file specified in the URI was not found on the remote system. ■ Remote storage is currently connected via KVMS – If the remote host storage device is connected to the Remote System Console Plus then the host storage device can not be used. ■ Remote target not available – The path to the virtual storage device image is not valid. ■ URI not configured – The remote server URI was not set. ■ URI not valid for requested operation – The remote server URI is not valid. ■ Username or password not configured (Samba only) – The user name or password was not set.
		CLI Syntax for status: Single server: <pre>show /SP/services/kvms/host_storage_device status</pre> Multi-domain server: <pre>show /Servers/PDomains/PDomain-n/SP/services/kvms/host_storage_device status</pre>

▼ Uploading a New Solaris Miniroot Package From SP to Host

Use the Miniroot properties in Oracle ILOM to manage the Solaris Miniroot package that is currently installed on a host server. Supported management actions include:

- Viewing the Solaris Miniroot version installed on the host server.
- Recovering an existing Solaris Miniroot image on a host server by uploading a new Solaris Miniroot package to the SP and connecting it automatically to the host server.

Before You Begin

- The Admin (a) role is required to load a new version of the Solaris Miniroot package on the SP.
- Oracle ILOM firmware release 3.2.5.5 or later must be installed on one of the following: 1) SPARC M7 series server, 2) SPARC T7 series server, or 3) next generation SPARC series servers such as SPARC S7-2L servers or T8 series servers.
- The Miniroot feature applies only to SPARC servers with a pre-installed Solaris Miniroot image.
- To automatically connect the new miniroot.iso file to the host server, the Mode property on the Remote Control > Host Storage Device page must be set to Miniroot.
- The Host Management > Keyswitch property in Oracle ILOM must be set to Normal. Otherwise, if the Keyswitch property is set to Locked, the Load button on the Miniroot page will be disabled.
- The System Management Miniroot properties are accessible from the active SP. The host storage redirection mode is set on the Host Storage Device page (or the host_storage_device CLI target).
- For information about how to update the Solaris mini-root image, see the instructions for "How to Update the Fallback Mini-root Image" in the Solaris documentation (https://docs.oracle.com/cd/E53394_01/html/E54742/gplct.html#scrolltoc).

Follow these steps to manage the Solaris Miniroot package from the Oracle ILOM SP web interface:

Note - For Miniroot CLI properties, see “[System Management Miniroot Property Descriptions](#)” on page 162, as well as the Mode property that is described in “[CLI and Web Host Storage Device Properties](#)” on page 157.

1. **To view the version of the Solaris Miniroot image installed on the managed server, perform the following:**
 - **In the Oracle ILOM web interface, click System Management > Miniroot.**
The installed version of the Solaris Miniroot package installed on the managed server appears on the Miniroot page.
2. **To upload a new Solaris Miniroot package to the SP and have it automatically connect to the host server, perform the following:**
 - a. **Navigate to the Remote Control > Host Storage Device page to ensure that the Mode property is set to Miniroot.**
For instructions on how to modify the Mode property on the Remote Control > Host Storage Device page, click the More details ... link.

- b. To upload a new Solaris Miniroot package to the SP and have it automatically connect to the host server, perform these steps:
- i. Navigate to the System Management Miniroot page and click the Load Miniroot Package button.
The Miniroot Update page appears.
 - ii. In the Miniroot Update page, perform the following:
 - Click either the Local File Browse button or specify a URL to locate the new Solaris Miniroot package.
 - Click Upload.
A confirmation message appears indicating the upload is complete and an SP reset is not necessary. The newly uploaded Solaris miniroot.iso file is automatically connected to the host on the managed server.

System Management Miniroot Property Descriptions

User Interface Configurable Target:

- CLI: `/SP/firmware/host/miniroot`
- Web: System Management > Miniroot
- User Role: admin (a) (required for property modification)

Property	Description
Miniroot Version (version=)	The Miniroot version is a read-only property that identifies the installed version of the Solaris Miniroot package on the managed server. CLI Create User Syntax: show /SP/firmware/host/miniroot version=
Load Miniroot Package (button) (load_uri=)	The Load button or the <code>load_uri</code> target enables you to specify the location of the new Solaris Miniroot package. CLI Syntax to Load Miniroot Package: load /SP/firmware/host/miniroot load_uri=file_transfer_method://host_address/file_path/minroot.iso_filename Where <code>file_transfer_method</code> can include: TFTP FTP SFTP SCP HTTP HTTPS Paste.

User Interface Configurable Target:

- CLI: /SP/firmware/host/miniroot
- Web: System Management > Miniroot
- User Role: admin (a) (required for property modification)

Property	Description
	For a detailed description of each file transfer method (excluding Paste), see “Supported File Transfer Methods” on page 50 .

Connecting to the Oracle ILOM Remote System VNC Console

Note - The Oracle ILOM Remote System VNC Console is supported on all newly released SPARC servers that shipped with Oracle ILOM firmware version 3.2.6 or later.

The Oracle ILOM Remote System VNC Console is an implementation of the Virtual Network Computing (VNC) system. It enables you to remotely redirect the host server keyboard, video, and mouse (KVM) events to a graphical shared desktop display.

To establish an Oracle ILOM Remote System VNC Console connection to the Solaris VNC server over the internal Local Host Interconnect interface, you must launch a VNC viewer from your desktop and specify the server SP hostname or IP address as the remote VNC server. For further configuration details, see the following information:

- [“Before You Begin” on page 163](#)
- [“Establishing an Oracle ILOM Remote System VNC Console Connection” on page 165](#)
- [“Troubleshooting the VNC Connection” on page 166](#)

Before You Begin

- The following software requirements must be met on the managed SPARC host server:
 - Oracle ILOM firmware version 3.2.6 or later must be installed on the SPARC server (SPARC S7-2, M7, T7, and next generation series SPARC servers).
 - One of the following Oracle Solaris operating systems must be installed on the SPARC server:
Oracle Solaris 11.2 SRU8, Oracle Solaris 11.3 or later
 - The solaris-desktop package must be installed on the host server using the Solaris Image Packing Systems (IPS). For further information about using IPS, refer to the Solaris user documentation for adding and updating Oracle Solaris packages.

Note - After the installation of the `solaris-desktop` package, the xVNC server is enabled by default on the Solaris host server.

- The following VNC viewer requirements must be met on the management station:
 - A VNC viewer, supporting TLS 1.1 or 1.2 encryption, must be installed.
For instance, TigerVNC is a VNC viewer that supports the required TLS encryption in both Windows and Linux environments.

Note - The TLSv 1.1 property in Oracle ILOM is disabled by default as of Oracle ILOM 4.0.4.

- A single Oracle ILOM Remote System VNC Console connection to the Oracle Solaris host VNC server is allowed at one-time.
- The following properties in Oracle ILOM must be enabled:
 - The KVMS `servicestate` property in Oracle ILOM must be set to enabled. This property is enabled by default. If required, a user with Admin role privileges can enable this property from the command line by typing:
 - The Local Host Interconnect `hostmanaged` property must be set to True (default setting) and the `state` property should be set to disabled (default setting) in Oracle ILOM. If required, a user with Admin role privileges can set these property from the command line by typing:

```
set /SP/services/kvms servicestate=enabled
```

```
set /SP/network/interconnect state=disabled hostmanaged=true
```

Note - Oracle ILOM will auto-configure the Ethernet-over-USB connection points when the `state` property is set to disabled (default setting) and the `hostmanaged` property is set to true (default setting).

Note - If you set the state property to enabled or the hostmanaged property to false after an interconnect management connection is automatically established by Oracle ILOM, the hosts applications currently running on the internal interconnect management connection will fail to run. For more information about configuring the Local Host Interconnect feature in Oracle ILOM, see [“Dedicated Interconnect SP Management Connection” on page 24](#).

▼ Establishing an Oracle ILOM Remote System VNC Console Connection

Follow these steps to establish an Oracle ILOM Remote System VNC Console connection to the remote Oracle Solaris VNC server.

1. **Ensure that all the requirements described in the [“Before You Begin” on page 163](#) section have been met.**
2. **Launch an Oracle ILOM Remote System VNC Console connection from the local desktop to the Solaris host VNC server using a VNC viewer.**

For instance, if you are using TigerVNC, you can launch the VNC viewer and establish a connection to Solaris host VNC server using either the command line or the Windows Start menu.

- **Command Line:**

`vncviewer [server SP hostname or IP address]`

-or-

`vncviewer [server SP hostname or IP address] :5900`

- **Windows Start Menu:**

1. Click the Start menu, select TigerVNC.
2. In the VNC Server property, type the server SP address (hostname or IP).
3. Click Connect.

Troubleshooting the VNC Connection

Follow these guidelines for troubleshooting the VNC connection to the Solaris host VNC server.

- **Verify the Xvnc on the Solaris host server is running.**

```
svcs -a |grep vnc
```

- **Restart Xvnc if reported disabled.**

```
svcadm enable svc:/application/x11/xvnc-inetd:default
```

Using the Oracle ILOM Remote System Console or Storage Redirection CLI

Note - The Oracle ILOM Remote System Console and the Oracle ILOM Storage Redirection CLI features are available on all of Oracle systems that upgraded from Oracle ILOM 3.0.x to 3.1.x or from Oracle ILOM 3.1.x to 3.2.1 or later.

Description	Links
Refer to these sections for setting up and using the GUI-based Oracle ILOM Remote System Console for host server KVMS redirection.	■ “Oracle ILOM Remote System Console ” on page 168 ■ “Remote System Console First-Time Setup ” on page 168 ■ “Launching and Using the Oracle ILOM Remote System Console” on page 176 ■ “Remote System Console Menu Options, Usage Considerations, and Toggle Keys ” on page 178 ■ “International Keyboard Support” on page 181
Refer to these sections for setting up and using the text-based Oracle ILOM Storage Redirection CLI feature.	■ “Oracle ILOM Storage Redirection CLI” on page 181 ■ “Storage Redirection CLI First-Time Setup” on page 181 ■ “Launching and Using the Oracle ILOM Storage Redirection CLI” on page 188 ■ “Storage Redirection Commands and Options” on page 192 ■ “Resolving Warning Messages for Self-Signed SSL Certificate ” on page 216 ■ “Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate” on page 218

Related Information

- *Oracle ILOM Security Guide (3.2.x)*, Using Remote KVMS Securely

Oracle ILOM Remote System Console

The Oracle ILOM Remote System Console is available on all Oracle systems that upgraded from Oracle ILOM 3.0.x to 3.1.x or from Oracle ILOM 3.1.x to 3.2.1 or later.

The Oracle ILOM Remote System Console enables system administrators to remotely redirect host server system devices such as keyboard, video, mouse, and storage. The Oracle ILOM Remote System Console offers both a serial-line redirection option and a video redirection option:

- **Serial Line Redirection** (Oracle's SPARC servers only) — The serial line redirection option supports a single full-control text-based console session per server SP.
- **Video Redirection** (all Oracle systems) — The video redirection option supports one or more full-control graphic console sessions per server SP.

Note - If you received a newly released Oracle server with Oracle ILOM firmware 3.2.1 or later installed, see [“Using the Oracle ILOM Remote System Console Plus” on page 197](#).

For further details about setting up or using the Oracle ILOM Remote System Console, see these topics:

- [“Remote System Console First-Time Setup ” on page 168](#)
- [“Optionally Set a Lock Mode to Secure the Host Server Desktop ” on page 173](#)
- [“Launching and Using the Oracle ILOM Storage Redirection CLI” on page 188](#)
- [“Remote System Console Menu Options, Usage Considerations, and Toggle Keys ” on page 178](#)

Remote System Console First-Time Setup

To set up the Oracle ILOM Remote System Console for first-time use, refer to these topics:

- [“Requirements for Using the Oracle ILOM Remote System Console” on page 169](#)
- [“Configure Local Client KVMS Settings” on page 170](#)
- [“Register 32-Bit JDK Java Plug-In For Windows IE Web Browser” on page 172](#)
- [“Register 32-Bit JDK Java Plug-In for Mozilla Firefox Web Browser” on page 172](#)
- [“Optionally Set a Lock Mode to Secure the Host Server Desktop ” on page 173](#)

Requirements for Using the Oracle ILOM Remote System Console

The following requirements must be met prior to using the Oracle ILOM Remote System Console for the first time:

TABLE 56 Requirements for Using Oracle ILOM Remote System Console

Set Up Requirement	Description
Firmware	The Oracle ILOM Remote System Console is available on all servers that shipped with Oracle ILOM 3.0.x or Oracle ILOM 3.1.x or have been upgraded from Oracle ILOM 3.0.x or Oracle ILOM 3.1.x to Oracle ILOM 3.2.1 or later.
KVMS Settings	Configure the SP local client properties for keyboard, video, and mouse redirection behavior. KVMS Defaults: State: Enabled, Mouse Mode: Absolute, Display Quality: YUV420, Lock Mode: Disabled Related Information: ■ “Configure Local Client KVMS Settings” on page 170
Java Runtime Environment	The Oracle ILOM Remote System Console requires the Java Runtime Environment to be either Java 7 update 131 or later, Java 8, or Java 9. To download the latest Java Runtime Environment, go to http://java.com. Note - All Java versions support TLS v1.2. However, if a version <i>prior</i> to Java 7u131 is installed, you will need to manually enable TLS v1.2, or update your system with a later Java version. For information about configuring TLS properties in Oracle ILOM, see Table 38, “Web Server Configuration Properties,” on page 101.
Required JDK and Web Browser	■ For IPv4 networks, the 32-bit JDK is required. ■ For IPv6 networks, the JDK170b36 or higher is required. For supported web browsers, see “Supported Web Browsers for Oracle ILOM” on page 40.
Registration of 32-bit JDK for Video Redirection	The 32-bit JDK Java Plug-in must be registered with the local client web browser prior to using the Oracle ILOM Remote System Console for video redirection. Related Information: ■ “Register 32-Bit JDK Java Plug-In For Windows IE Web Browser” on page 172 ■ “Register 32-Bit JDK Java Plug-In for Mozilla Firefox Web Browser” on page 172
User Roles and Host Server User Credentials	■ The Admin (a) role is required in Oracle ILOM to modify the KVMS service State. ■ The Console (c) role is required in Oracle ILOM to modify KVMS properties (excluding the State property) and to launch the Oracle ILOM Remote System Console. ■ Host server user credentials are required to access the redirected host server.
Video Redirection and Serial Redirection Use	When launching the Oracle ILOM Remote System Console, users can launch the remote KVMS session using one of the following redirection methods: ■ Serial Redirection (Oracle SPARC servers only) – This option is available for Oracle SPARC server SPs only. When enabled, Oracle ILOM presents a text-based console for serial host server redirections.

Set Up Requirement	Description
	■ Video Redirection – This option is available for Oracle's CMMs, x86 server SPs, and SPARC server SPs. This option presents a GUI-based console for the video redirected host server.
Communication TCP/IP Ports Required	The Oracle ILOM Remote System Console uses the following TCP/IP communication ports by default: ■ Port: 5120 for CD redirection ■ Port: 5123 for floppy redirection ■ Port: 5556 for user authentication redirection ■ Port: 7578 for video redirection ■ Port: 7579 for Oracle SPARC server redirection only For a complete list of default network ports, see “Default Network Ports Used by Oracle ILOM” on page 99.
Trusted SSL Certificate Support	As of Oracle ILOM firmware version 3.2.8, additional certificate checks will occur if the self-signed Default SSL Certificate is in use. For further information about resolving certificate warning messages for a default SSL certificate, see: “Resolving Warning Messages for Self-Signed SSL Certificate” on page 216. As of Oracle ILOM firmware 3.2.10, additional custom certificate checks will occur if the custom SSL certificate and private key are not properly configured. For instance: ■ A custom Certification Authority (CA) SSL Certificate and a Private Key are upload to Oracle ILOM. ■ The Java Keystore on the client side is not properly configured with the required root CA certificate to validate the uploaded custom SSL certificate and private key in Oracle ILOM. For further information about resolving warning messages for Custom SSL Certificates, see “Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate” on page 218.

▼ Configure Local Client KVMS Settings

1. **To access the server SP KVMS settings in Oracle ILOM, perform one of the following:**
 - **For Oracle single-server SP systems:**

Web – Click Remote Console > KVMS > KVMS Settings.

CLI – Type `show /SP/services/kvms`
 - **For Oracle multi-domain SP systems:**

Web – Select a Domain from the Manage list box then click Remote Console > KVMS > KVMS Settings.

CLI – Type `show /Servers/PDomains/PDomain_n/SP/services/kvms`
2. **Modify the following KVMS properties as required:**

Property	Description
State (servicestate=)	The KVM service State is enabled by default for redirection. This State property must be enabled for you to use the Oracle ILOM Remote System Console. If the State property is disabled, you will not be able to use the Oracle ILOM Remote System Console. CLI Syntax for KVM Service State: - Single Server SP: set /SP/services/kvm servicestate=enabled disabled - Multi-domain server SP: set Server/Pdomains/PDomain_n/SP/services/kvm servicestate=enabled disabled
Mouse Mode (mousemode=)	Set the appropriate Mouse Mode option from the list below: - Relative (default) – Set this local Mouse Mode if your remote host is running a Linux OS. - Absolute – Set this local Mouse Mode if your remote host is running a Windows or Solaris OS. CLI Syntax for KVM Mouse Mode: - Single-server SP: set /SP/services/kvm mousemode=absolute relative - Multi-domain server SP: set /Servers/Pdomains/PDomain_n/SP/services/kvm mousemode=absolute relative
Display Quality (display_quality=)	Select the appropriate video Display Quality option from the list below: - YUV420 (initial factory default) – Select this setting to transmit a more highly compressed color image data scheme, resulting in an optimized data transfer rate. - YUV444 – Select this setting to transmit a less-compressed color image data scheme, resulting in a greater image resolution. - VQ2 – Select this setting to transmit a less-compressed video data scheme that works best for two-color terminal display outputs. - VQ4 – Select this setting to transmit a less-compressed video data scheme that works best for four-color terminal display outputs. Note - The Display Quality value you set remains persistent after you reboot the SP. Therefore, the initial factory default value (YUV420) is not retained if modifications are made. CLI Syntax for KVM Display Quality: Single-server SP:

Property	Description
	<code>set /SP/services/kvms display_quality=YUV420 YUV444 VQ2 VQ4</code> Multi-domain server SP: <code>set /Servers/Pdomains/PDomain_n/SP/services/kvms display_quality=YUV420 YUV444 VQ2 VQ4</code>
Host Lock Mode (lockmode=)	For a description of the host lock properties, see “Optionally Set a Lock Mode to Secure the Host Server Desktop” on page 173.

3. To apply modifications, click Save on the KVMS Settings page.

▼ Register 32-Bit JDK Java Plug-In For Windows IE Web Browser

1. On the Windows Client, open Windows Explorer (not Internet Explorer).
2. In the Windows Explorer dialog box, click Tools > Folder Options, and then click the Files Types tab.
3. In the Files Types tab, do the following:
 - a. In the Registered File Type list, select the JNLP file type and click Change.
 - b. In the Open With dialog box, click Browse to select the 32-bit JDK file.
 - c. Select the “Always use the selected program to open this kind of file” check box.
 - d. Click OK, and then launch the Oracle ILOM Remote System Console.
For instructions, see [“Launching and Using the Oracle ILOM Remote System Console”](#) on page 176.

▼ Register 32-Bit JDK Java Plug-In for Mozilla Firefox Web Browser

1. Launch the Oracle ILOM Remote System Console from the Oracle ILOM web interface.

Click Remote Console > Redirection.

In the Launch Redirection page, choose a serial or video redirection method if presented, and then click the Launch Remote System Console button.

Note - Alternatively, the Oracle ILOM Remote System Console is accessible from the Actions Panel on the Summary page in the web interface.

A dialog box for the Java Start Web Program appears.

2. **In the Java Start Web Program dialog box, do the following:**
 - a. Click “Open with...” to specify the location of the 32-bit JDK file.
 - b. Select the “Do this automatically for files like this from now on” check box.

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

The Oracle ILOM Remote System Console window appears.

For further information on how to redirect KVMS devices using the Oracle ILOM Remote System Console, see [“Launching and Using the Oracle ILOM Remote System Console” on page 176](#).

Optionally Set a Lock Mode to Secure the Host Server Desktop

Oracle ILOM provides the option to lock the host server desktop whenever a remote KVMS session disconnects. This feature ensures that if a KVMS session user closes the session prior to logging out of the host server desktop, subsequent KVMS session users will be prompted to enter their user credentials to gain access to the system.

For a description of lock mode options, as well as instructions for configuring the lock mode in Oracle ILOM, see the following information:

- [Table 57, “Configurable Host Server Lock Options ,” on page 174](#) Configurable Host Server Lock Options
- [“Lock Host Desktop When Disconnecting a Remote KVMS Session” on page 174](#)

TABLE 57 Configurable Host Server Lock Options

Lock Mode Property Values	Description
Windows (lockmode=windows)	The Windows Lock Mode setting is configurable for host servers running a Microsoft Windows operating system. When the host Lock Mode property is set to Windows, Oracle ILOM works in conjunction with the standard Windows keyboard shortcut (Ctrl+Alt+Del K) for locking the Windows operating system desktop.
Custom (lockmode=custom)	The Custom Lock Mode setting is configurable for host servers running an Oracle Solaris operating system, a Linux-based operating system, or a Microsoft Windows operating system without using the Ctrl+Alt+Del K key sequence. When the host Lock Mode property in Oracle ILOM is set to Custom, Oracle ILOM supports the use of the following key sequences to lock the desktop: ■ A custom key sequence supported by Oracle Solaris or a Linux-based operating system. The custom key sequence needs to be defined on the host operating system prior to enabling the Custom Lock Mode setting in Oracle ILOM. For instructions for creating a custom key sequence, refer to the operating system vendor documentation. ■ A custom key sequence supported by Windows such as the Windows Logo Key+L keyboard shortcut. The Custom Lock Mode option in Oracle ILOM does not support the standard Windows keyboard shortcut for locking the desktop (Ctrl+Alt+Del K).
Disabled (lockmode=disabled)	When the host Lock Mode property is set to Disabled (default), Oracle ILOM will not automatically lock the host server desktop when a remote KVMS session ends.

▼ Lock Host Desktop When Disconnecting a Remote KVMS Session

Before You Begin

- For Custom Lock Mode configurations, the custom key sequence must be defined on the host server operating system prior to setting the Custom Lock Mode option in Oracle ILOM.
 - The Console (c) role is required to modify the host lock properties in Oracle ILOM.
1. **Set a value for the Host Lock Mode property in Oracle ILOM by doing the following:**
 - **Web – Click Remote Control > KVMS. In KVMS Settings page, click the Lock Mode list box to select one of the following values: Windows, Custom, or Disable.**
 - **CLI – Type:**

```
set /SP/services/kvms lockmode=windows|custom|disabled
```

If you set the Lock Mode property to Custom, proceed to Step 2. If you did not set the Lock Mode property to Custom and you are using the web interface, proceed to Step 3. Otherwise, you have completed the procedure.

2. If the Lock Mode property in Step 1 was set to Custom, perform the following steps to specify Custom Lock Modifiers and a Custom Lock key:

■ **Web – In the KVMS Settings page do the following:**

- a. Click the Custom Lock Modifiers list box and select the custom key sequence defined on the host server OS.
- b. Click the Custom Lock Key list box and select a custom lock key.

■ **CLI – Type:**

- a. `set /SP/services/kvms lockmodifiers=value`
- b. `set /SP/services/kvms custom_lock_key=value`

Possible Custom Lock Modifiers Values: l_alt, r_alt, l_shift, r_shift, l_ctrl, r_ctrl, l_gui, r_gui

Up to four Custom Lock Modifiers values can be specified. Each modifier can be separated by a comma.

Possible Custom Lock Key Values: esc, end, tab, ins, del, home, enter, space, break, backspace, pg_up, pg_down, scr_lck, sys_rq, num_plus, num_minus, f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, a-z, 0-9, !, @, #, \$, %, ^, &, *, (,), -, _, =, +, ?, |, ~, [, {,], }, ;, :, <, ., >, /

See the Host Lock Configuration Example following this procedure.

3. To apply the property changes you made within the KVMS Setting page, click Save.

Host Lock Configuration Example:

If Shift+Control+Backspace was defined on the host server operating system as a custom lock key sequence, then the following KVMS lock properties would be set in the Oracle ILOM SP:

```
/SP/services/kvms
Properties:
  custom_lock_key = backspace
```

```
custom_lock_modifiers = l_shift, l_ctrl
lockmode = custom
mousemode = absolute
servicestate = enabled
```

Launching and Using the Oracle ILOM Remote System Console

For instructions for launching and using the web-based Oracle ILOM Remote System Console, see these topics:

- [“Launch and Use the Oracle ILOM Remote System Console” on page 176](#)
- [“Remote System Console Menu Options, Usage Considerations, and Toggle Keys” on page 178](#)

▼ Launch and Use the Oracle ILOM Remote System Console

Before You Begin

- Ensure that the requirements for first-time use have been met: [Table 56, “Requirements for Using Oracle ILOM Remote System Console,” on page 169.](#)
- Console (c) user role privileges are required to use the Oracle ILOM Remote System Console and the Oracle ILOM Remote System Console Plus.
- Upon launching the Remote Control > Redirection page, a serial redirection and a video redirection option are presented for Oracle SPARC server SPs only. For Oracle x86 server SPs, the video redirection option is used by default.
- Solaris users must use the serial-redirection mode in Oracle ILOM Remote System Console to access the Solaris Host Console, view Solaris Host Console messages, or to issue Solaris Host Console commands such as boot commands. The video mode redirection option in the Oracle ILOM Remote System Console must not be used to access the Solaris Host Console, view Solaris Host Console messages, or to issue Solaris Host Console commands such as boot commands.
- To control the use of the keyboard and mouse between the Oracle ILOM Remote System Console and the host desktop, see [“Toggle Key Sequence for Keyboard and Mouse Control” on page 181.](#)
- Upon establishing a redirection session to the host server, user credentials are required to log in to the host operating system desktop.

1. To launch the Oracle ILOM Remote System Console, do the following:

- a. In the Oracle ILOM web interface, click Remote Console > Redirection.**

Note - Alternatively, SP and CMM users can launch the Oracle ILOM Remote System Console from the Actions panel on the Summary page.

- b. In the Launch Redirection page, click a redirection option if options are presented, and then click the Launch Remote Console button.**

The redirected host server desktop appears in its present state. For instance, if the host server is powering on, a set of boot messages appear; if the host server operating system is powered-on, a desktop login dialog appears; if the host server is not powered-on, a blank screen appears.

Note - If Oracle ILOM firmware 3.2.8 or later is installed and a Warning message (Check Certificate or Video Redirection Error) appears prior to launching the Oracle ILOM Remote System Console, see [“Resolving Warning Messages for Self-Signed SSL Certificate” on page 216](#).

2. To stop, restart, or start a new redirection session, click the Redirection menu and select the appropriate menu option.

For a description of menu options, see [“Redirection Menu Options” on page 178](#).

Special Considerations:

- A single redirection view automatically appears when the KVMS session is launched from a single host server SP.
- Multiple redirection views are possible when: (1) a new KVMS session is manually added; or (2) when the initial KVMS session is launched from the chassis monitoring module (CMM) web interface. A CMM KVMS session presents one redirection view for each chassis-managed CPU blade server SP.

3. To redirect devices, click the Devices menu and select the appropriate menu option.

For a description of menu options and special considerations for redirecting storage media, see [“Devices Menu Options ” on page 179](#).

4. To set keyboard modes and send options, click the Keyboard menu and select the appropriate menu option.

For a description of menu options, see [“Keyboard Menu Options” on page 180](#).

5. To exit the Remote System Console, click Quit in the Redirection menu.

Related Information

- [“Requirements for Using the Oracle ILOM Remote System Console” on page 169](#)
- [“Remote System Console Menu Options, Usage Considerations, and Toggle Keys ” on page 178](#)
- [“Optionally Set a Lock Mode to Secure the Host Server Desktop ” on page 173](#)
- [“Storage Redirection CLI First-Time Setup” on page 181](#)

Remote System Console Menu Options, Usage Considerations, and Toggle Keys

Refer to these topics for descriptions of Oracle ILOM Remote System Console menu options, device redirection considerations, and toggle key usage.

- [“Redirection Menu Options” on page 178](#)
- [“Devices Menu Options ” on page 179](#)
- [“Device Redirection Usage Considerations” on page 179](#)
- [“Keyboard Menu Options” on page 180](#)
- [“Toggle Key Sequence for Keyboard and Mouse Control ” on page 181](#)
- [“International Keyboard Support” on page 181](#)

Redirection Menu Options

Menu Option	Description
Start Redirection (enabled by default)	Click Start Redirection to enable redirection service. This option is enabled by default; therefore, the redirection service is automatically started when you launch the Oracle ILOM Remote System Console.
Restart Redirection	The Restart Redirection option stops and starts the active keyboard, video, mouse, and storage redirection.
Stop Redirection	The Stop Redirection option stops the active keyboard, video, mouse, and storage redirection.
New Session	A new redirection session is added to the current tab set.
Delete Session	A redirection session is deleted from the current tab set.

Devices Menu Options

Devices Menu Option	Description
Keyboard (enabled by default)	Click Keyboard to turn on or turn off the redirection service for the local client keyboard. This option is enabled by default; therefore, the redirection service is automatically started for the local client keyboard.
Mouse (enabled by default)	Click Mouse to turn on or turn off the redirection service for the local client mouse. This option is enabled by default; therefore, the redirection service is automatically started for the local client mouse.
CD-ROM	Click CD-ROM to enable the local CD device to behave as if it were directly attached to the remote host server.
Floppy	Choose Floppy to enable the local floppy device to behave as if it were directly attached to the remote host server. This option is not supported on Oracle SPARC host servers.
CD-ROM Image	Choose CD-ROM Image to specify the location of a CD-ROM image file that is stored on the local client or on a network share.
Floppy Image	Choose Floppy Image to specify the location of a floppy image file that is stored on the local client or on a network share. This option is not supported on Oracle SPARC host servers.
Save as host defaults	Click Save as host defaults to set the Devices menu options that are selected as the default settings.

Device Redirection Usage Considerations

- If you are installing software from a distribution media (such as a CD or DVD), ensure that the media is inserted in the redirected drive on the local client.
- If you are installing software from an ISO image, ensure that the ISO image is stored on the local client or on a shared network file system.
- Oracle Solaris client users must perform the following actions prior to redirecting storage devices:
 - If Volume Manager is enabled, you will need to disable this feature.
 - Log in as `root` to start storage redirection.

Alternatively, to start storage redirection, you can assign `root` privileges to the processor that is running the Oracle ILOM Remote System Console by entering these commands:

```
su to root
```

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

Keyboard Menu Options

Note - For a list of supported keyboard languages, see [“International Keyboard Support” on page 181](#)

Keyboard Menu Option	Description
Auto-Keybreak Mode (enabled by default)	Select Auto-Keybreak Mode to automatically send a key break after every keystroke. This option can be helpful for resolving keyboard problems over slow network connections.
Stateful Key Locking	This option applies to Oracle Solaris with Xsun or OSX. Select Stateful Key Locking if the local client uses stateful key locking. Stateful key locking applies to these three lock keys: Caps Lock, Num Lock, and Scroll Lock.
Left Alt Key	This option is not available on Windows clients. Select Left Alt Key to turn on or turn off the left Alt key.
Right Alt Key / Alt Graph Key	This option applies to non-US keyboards. Click Right Alt Key (Alt Graph Key) to toggle the right Alt key on or off. When selected, this option enables you to type the third key character on a key.
F10	Click F10 to apply the F10 function key. This option typically applies to the BIOS functionality on Oracle x86 host servers.
Control Alt Delete	Click Control Alt Delete to send the Ctrl+Alt+Del sequence.
Control Space	Click Control Space to send a Control+Space sequence to the host server, which enables keyboard input.
Caps Lock	Click Caps Lock to send the Caps Lock key to the host server, which enables input from Russian and Greek keyboards.

Toggle Key Sequence for Keyboard and Mouse Control

Use one of the following toggle key sequences to shift control of the keyboard and mouse between the Oracle ILOM Remote System Console application and the local client desktop.

Local Client Device	Toggle Key Sequence
Mouse	Alt-m
Keyboard	Alt-k

International Keyboard Support

The Oracle ILOM Remote System Console supports the use of the following international keyboard language layouts:

■ Brazilian-Portuguese	■ French	■ Japan (JP) Note: Only in English mode.
■ Chinese	■ German	■ Russian
■ Chinese -Traditional (Taiwan)	■ Italian (IT)	■ Turkish
■ English (US)	■ Korean	
■ Estonian	■ Spanish	

Oracle ILOM Storage Redirection CLI

The Oracle ILOM Storage Redirection CLI feature is available on all Oracle systems that upgraded from Oracle ILOM 3.0.x to 3.1.x or from Oracle ILOM 3.1.x to 3.2.1 or later.

The Oracle ILOM Storage Redirection CLI enables system administrators to remotely redirect storage devices on host server systems. For details about setting up and using the Oracle ILOM Storage Redirection CLI feature, see these topics:

- [“Storage Redirection CLI First-Time Setup” on page 181](#)
- [“Launching and Using the Oracle ILOM Storage Redirection CLI” on page 188](#)

Storage Redirection CLI First-Time Setup

To set up the Oracle ILOM Storage Redirection for first-time use, refer to these topics:

- “Requirements for Using the Oracle ILOM Storage Redirection CLI” on page 182
- “Register Java Plug-In for Windows IE Browser and Start Service for First Time” on page 183
- “Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser” on page 184
- “Install the Storage Redirection Client” on page 185
- “Optionally Modify the Default Network Port 2121 for Storage Redirection” on page 186

Requirements for Using the Oracle ILOM Storage Redirection CLI

The following requirements must be met prior to using the Oracle ILOM Storage Redirection CLI for the first time:

TABLE 58 Requirements for Using Oracle ILOM Storage Redirection CLI

Setup Requirement	Description
JRE 1.5 environment	The storage redirection service and client are Java Web Start applications that require the installation of the Java Runtime Environment (1.5 or later) on the local client system. To download the latest Java Runtime Environment (JRE), see http://java.com.
Register 32-Bit JDK Plug-in and Start Storage Redirection Service	The storage redirection service must be installed locally or set to run from the Oracle ILOM web interface. The 32-bit JDK Java plug-in must also be registered with the local client web browser. Related Information: ■ “Register Java Plug-In for Windows IE Browser and Start Service for First Time” on page 183 ■ “Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser” on page 184
Install Storage Redirection Client	After registering the 32-bit JDK plug-in with the local client web browser and starting the storage redirection service for the first-time, the storage redirection client must be installed on the local client system. Related Information: ■ “Install the Storage Redirection Client” on page 185
User Roles	A Console (c) role is required in Oracle ILOM to launch and use the Oracle ILOM Storage Redirection CLI.
Communication TCP/IP Port Required	The Oracle ILOM Storage Redirection CLI, by default, uses TCP/IP port: 2121 to communicate with the host server. Related Information: ■ “Optionally Modify the Default Network Port 2121 for Storage Redirection” on page 186

▼ Register Java Plug-In for Windows IE Browser and Start Service for First Time

Perform this procedure to: (1) register the 32-bit JDK Java plug-in with the Microsoft Windows IE browser, and (2) start the storage redirection service for the first time.

1. **On the local Windows client, open Windows Explorer (not Internet Explorer).**
2. **In the Windows Explorer dialog box, click Tools > Folder Options, and then click the Files Types tab.**
3. **In the Files Types tab, do the following:**
 - a. **In the Registered File Type list, select the JNLP file type and click Change.**
 - b. **In the Open With dialog box, click Browse to select the 32-bit JDK file stored on the local client system.**
 - c. **Enable the check box for “Always use the selected program to open this kind of file.”**
 - d. **Click OK.**
4. **To start the storage redirection service for the first time, open the Oracle ILOM web interface, and then click Remote Control > Redirection > Launch Service.**

The Opening Jnlpgenerator-cli dialog box appears.
5. **In the Opening Jnlpgenerator-cli dialog box, choose one of the following options to either install the file or run it from the web interface:**
 - **Install – Click “Save to disk,” specify a storage file location, and then click OK.**
 - **Run – Click “Open it with,” choose the `javaws` (default) 32-bit JDK file on the local system, and then click OK. The Security Warning dialog box appears prior to running the storage redirection service.**

Special Considerations:

- If you choose to run the `Jnlpgenerator-cli` file instead of installing the file, subsequent users will need to start the storage redirection service from the Oracle ILOM web interface prior to using the Oracle ILOM Storage Redirection CLI console.

- If you choose to run the `Jnlpgenerator-cli` file and you selected the check box for “Always perform this action when handling this file type,” the `Jnlpgenerator-cli` dialog box will become unavailable in the future and you will not be able to modify the default storage network port. Therefore, if in the future the default network port (2121) will need to be modified, you should not enable this check box.

6. Start the storage redirection service by performing one of the following:

- **If the `Jnlpgenerator-cli` file is installed locally:**

Type the location of the installed `Jnlpgenerator-cli` file, followed by the `javaws rconsole.jnlp` command to start the service.

Example Syntax:

```
cd jnlp_file_location javaws rconsole.jnlp
```

- **If the `Jnlpgenerator-cli` file is configured to run:**

In the Security Warning dialog box, click Run (or Yes) to start the service.

If the storage redirection service fails to start, an error message appears informing you of an error condition. If an error message did not appear, the service is started and is waiting for user input.

▼ Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser

Perform this procedure to: (1) start the storage redirection service for the first time, and (2) register the 32-bit JDK Java plug-in with the Mozilla Firefox web browser.

1. Launch the storage redirection service from the Oracle ILOM web interface.

Click Remote Control > Redirection > Launch Service.

A dialog box appears for opening the `Jnlpgenerator-cli` file.

2. In the Opening `Jnlpgenerator-cli` dialog box, choose one of the following options to install the service locally or run the service from the web interface:

- **Install – Click “Save to disk,” specify a storage file location, and then click OK.**

- **Run** – Click “Open it with,” choose the `javaws` (default) 32-bit JDK file on the local system, and then click OK. The Security Warning dialog box appears prior to running the storage redirection service.

Special Considerations:

- If you choose to run the `Jnlpgenerator-cli` file instead of installing the file, subsequent users will need to start the storage redirection service from the Oracle ILOM web interface prior to using the Oracle ILOM Storage Redirection CLI console.
- If you choose to run the `Jnlpgenerator-cli` file, and you select the check box for “Always perform this action when handling this file type,” the `Jnlpgenerator-cli` dialog box will become unavailable in the future and you will not be able to modify the default storage network port. Therefore, if in the future the default network port (2121) will need to be modified, you should not enable this check box.

3. Start the Storage Redirection Service by performing one of the following:

- **If the `Jnlpgenerator-cli` file is installed locally:**

Type the location of the installed `Jnlpgenerator-cli` file, followed by the `javaws rconsole.jnlp` command to start the service.

Example Syntax:

```
cd jnlp_file_location javaws rconsole.jnlp
```

- **If the `Jnlpgenerator-cli` file is configured to run:**

In the Security Warning dialog box, click Run (or Yes) to start the service.

If the storage redirection service fails to start, an error message appears informing you of an error condition. If an error message did not appear, the service is started and is waiting for user input

Related Information:

- [“Install the Storage Redirection Client” on page 185](#)
- [“Optionally Modify the Default Network Port 2121 for Storage Redirection” on page 186](#)

▼ Install the Storage Redirection Client

Perform the following procedure to install the storage redirection client on the local client system:

Note - This is a one-time client installation that needs to be completed before using the Oracle ILOM Storage Redirection CLI for the first time.

Before You Begin

- The Java plug-in should be registered and storage redirection service should be started for the first time.

For instructions, see either:

- [“Register Java Plug-In for Windows IE Browser and Start Service for First Time” on page 183](#)
- [“Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser” on page 184.](#)

To install the storage redirection client, perform these steps:

1. **In the Oracle ILOM web interface, click Remote Console > Redirection > Download Client.**

The Opening StorageRedir.jar file dialog box appears.

2. **In the Opening StorageRedir.jar dialog box, do the following:**

- Click “Save it to disk,” and then click OK.
- In the Save As dialog box, save the StorageRedir.jar file to a location on the local client system.

Related Information:

- [“Optionally Modify the Default Network Port 2121 for Storage Redirection” on page 186](#)
- [“Launching and Using the Oracle ILOM Storage Redirection CLI” on page 188](#)

▼ Optionally Modify the Default Network Port 2121 for Storage Redirection

Perform the following procedure to optionally modify the default network port 2121 used by Oracle ILOM for storage redirection.

Before You Begin

- The following procedure requires access to the `Jnlpgenerator-cli` file.

Note - If the `Jnlpgenerator-cli` file for the storage redirection service was previously configured to run from the web interface, and the Opening `Jnlpgenerator-cli` file dialog box was previously configured not to display, you will not be able to use the following procedure to change the default storage redirection network port.

- The Console (c) role is required to run the storage redirection service from the Oracle ILOM web interface.
- After modifying the default storage redirection port number, Oracle ILOM storage redirection users must always specify the non-default port number when starting, stopping, or viewing storage redirections from the command window or terminal.

To modify the default storage redirection network port 2121, follow these steps:

1. **To access the `Jnlpgenerator-cli` file, perform one of the following:**

- **If the storage redirection service `Jnlpgenerator-cli` file is installed:**
Open the locally stored `Jnlpgenerator-cli` file using a text editor.
- **If the storage redirection service `Jnlpgenerator-cli` file is set to run from web interface:**
 - a. **In the Oracle ILOM web interface, click Remote Control > Redirection > Launch Service.**
The Opening `Jnlpgenerator-cli` file dialog box appears.
 - b. **In the Opening `Jnlpgenerator-cli` dialog box, click “Save to disk,” and then click OK.**
 - c. **In the Save As dialog box, specify a location to store the file, and then click OK.**
 - d. **Using a text editor, open the `Jnlpgenerator-cli` file stored on the local client system.**

2. **Modify the port number argument referenced in the `Jnlpgenerator-cli` file, and then save the changes to the file.**

File example:

```
<application-desc>  
<argument>cli</argument>  
<argument>2121</argument>  
</application-desc>
```

After changing the default network port 2121 and saving the changes to the locally stored `Jnlpgenerator-cli` file, the non-default port number must always be specified when starting, stopping, or viewing storage redirections from the command window or terminal.

Launching and Using the Oracle ILOM Storage Redirection CLI

To launch and use the Oracle ILOM Storage Redirection CLI, see these topics:

- [“Launch the Oracle ILOM Storage Redirection CLI and Redirect Storage Devices” on page 188](#)
- [“Interactive and Non-Interactive Shell Syntax” on page 192](#)
- [“Storage Redirection Commands and Options” on page 192](#)

▼ Launch the Oracle ILOM Storage Redirection CLI and Redirect Storage Devices

Use the following procedure to launch and use the Oracle ILOM Storage Redirection CLI console:

Before You Begin

- Ensure that the requirements for first-time use have been met: [Table 58, “Requirements for Using Oracle ILOM Storage Redirection CLI,” on page 182.](#)
- The Console (c) role is required to launch and use the Oracle ILOM Remote System Console.
- Review the syntax for shell modes and the storage redirection commands:
[“Interactive and Non-Interactive Shell Syntax” on page 192](#)
[“Storage Redirection Commands and Options” on page 192](#)

To launch the Storage Redirection CLI and redirect storage devices, perform these steps:

1. To start the storage redirection service, perform one of the following:
 - Run the storage redirection service from the Oracle ILOM web interface as follows:
 - a. In the Oracle ILOM web interface, click **Remote Control > Redirection > Launch Service**.
The Opening Jnlpgenerator-cli file dialog box appears.
 - b. In the Opening Jnlpgenerator-cli dialog box, click “Open it with,” choose the javaws (default) 32-bit JDK file, and then click OK.
 - c. In the Security Warning dialog box, click **Run** to start the storage redirection service.
 - d. Open a command window or terminal on the local client system to launch the Oracle ILOM Storage Redirection CLI.
For Oracle ILOM Storage Redirection CLI launching instructions, see Step 2.
 - Start the (installed) storage redirection service from a command window as follows:
 - a. Open a command window or terminal on the local client system.
For example:
Windows systems: From the Start menu, click Run, type `cmd`, and then click OK.
Oracle Solaris or Linux systems: Open a terminal window on the desktop.
 - b. Navigate to the location where the `Jnlpgenerator-cli` file is installed, and then issue the `javaws rconsole.jnlp` command to start the service.
For example:

```
cd jnlp_file_location/javaws rconsole.jnlp
```
2. To launch the Storage Redirection CLI console from the command window or terminal, perform one of the following procedures based on the shell mode being used:

Shell Mode	Description and Procedure
Interactive shell mode	The interactive mode is useful when you need to enter a series of Storage Redirection commands.

Shell Mode	Description and Procedure
Non-interactive shell mode	To launch the Storage Redirection CLI using an interactive shell mode, perform these steps: 1. In the command-line interface, navigate to the directory where the storage redirection client (StorageRedir.jar) is installed using the <code>cd</code> command. For example: <code>cd my_settings/storage_redirect_directory</code> 2. Enter the following command to launch the Storage Redirection CLI: <code>java -jar StorageRedir.jar</code> For example: <code>C:\Documents and Settings\redirectstorage java -jar StorageRedir.jar</code> The <code><storageredir></code> prompt appears. Note - If you are using Windows, you must specify an uppercase letter for the target disk drive. For example, if the letter assigned to the target disk drive was <code>c</code>: you must specify <code>C</code>: instead of <code>c</code>. Tip - Enter only one space before <code>java</code> and one space before and after <code>-jar</code>. Otherwise, the <code>java -jar StorageRedir.jar</code> command will fail. Related Information: ■ “Interactive and Non-Interactive Shell Syntax” on page 192 The non-interactive mode is useful when you need to run a batch procedure or script. To launch the Storage Redirection CLI console using an non-interactive shell mode, perform these steps: 1. In the command-line interface, enter the command to launch the Storage Redirection CLI (<code>java -jar StorageRedir.jar</code>) at the shell prompt (<code>\$</code>). For example: <code>\$ java -jar StorageRedir.jar</code> 2. If the Storage Redirection CLI fails to launch, a detailed error message appears explaining the error condition. Otherwise, the Storage Redirection CLI is ready for user input. Note - You can launch multiple Storage Redirection CLI consoles by issuing the storage redirection command (<code>-jar StorageRedir.jar</code>) from a local command window or terminal. Tip - Enter only one space before and after <code>-jar</code>. Otherwise, the <code>java -jar StorageRedir.jar</code> command will fail. Related Information: ■ “Interactive and Non-Interactive Shell Syntax” on page 192 ■ “Storage Redirection Commands and Options” on page 192

3. To verify that the storage redirection service is running, type the following command:

test-service

A message appears stating whether the redirection service passed or failed.

For command descriptions and shell mode syntax, see these topics:

- [“Storage Redirection Commands and Options” on page 192](#)
- [“Interactive and Non-Interactive Shell Syntax” on page 192](#)

4. **To start storage redirection, type the following `start` command followed by the sub-commands and properties for the redirection device type, path to device, remote SP user name and password, and the IP address of the remote SP.**

For example:

Note - Commands shown in the following example should be entered as one continuous string.

```
start -r redir_type -t redir_type_path -u remote_username [-s remote_user_password] [-p  
non_default_storageredir_port] remote_SP_IP
```

For command descriptions and shell mode syntax, see these topics:

- [“Storage Redirection Commands and Options” on page 192](#)
- [“Interactive and Non-Interactive Shell Syntax” on page 192](#)

5. **To view active storage redirection, type the `list` command followed by the sub-commands and properties for any non-default storage redirection ports and the IP addresses of the remote host server SP.**

For example:

```
list [-p non_default_storageredir_port] remote_SP
```

For command descriptions and shell mode syntax, see these topics:

- [“Storage Redirection Commands and Options” on page 192](#)
- [“Interactive and Non-Interactive Shell Syntax” on page 192](#)

6. **To stop the redirection of a storage device, type the `stop` command followed by the commands and properties for the storage device type, remote SP user name and password, storage redirection port, and IP address of the remote host server SP.**

For example:

```
stop -r redir_type -u remote_username [-s remote_user_password] [-p  
non_default_storageredir_port] [-a yes/no] remote_SP
```

For command descriptions and shell mode syntax, see these topics:

- [“Storage Redirection Commands and Options” on page 192](#)
- [“Interactive and Non-Interactive Shell Syntax” on page 192](#)

7. **To display command-line Help, type the following command:**

help

The following information about the command syntax and usage appears.

Usage:

```
list [-p storageredir_port] [remote_SP]
start -r redir_type -t redir_type_path -u remote_username [-s remote_user_password]
[-a yes/no][[-p storageredir_port] remote_SP stop -r redir_type -u remote_username [-s
remote_user_password] [-a yes/no] [-p storageredir_port] remote_SP
stop-service [-p storageredir_port]
test-service [-p storageredir_port]
help
version
quit
```

Interactive and Non-Interactive Shell Syntax

The syntax required for entering the Storage Redirection commands in either of these modes is as follows:

- **Interactive shell mode syntax**

```
storageredir <command> <command_options> <sub_commands>
<sub_command_options>
```

- **Non-interactive shell mode syntax**

```
$ java -jar StorageRedir.jar <command> <command_options> <sub_commands>
<sub_command_options>
```

Storage Redirection Commands and Options

- [Table 59, “Storage Redirection Commands ,” on page 193](#)
- [Table 60, “Storage Redirection Command Options ,” on page 193](#)
- [Table 61, “Storage Redirection Sub-Commands ,” on page 193](#)
- [Table 62, “Storage Redirection Sub-Command Options ,” on page 194](#)

TABLE 59 Storage Redirection Commands

Command Name	Description
<code>java -jar StorageRedir.jar</code>	The <code>java -jar</code> command is used to launch the storage redirection client (<code>StorageRedir.jar</code>) from a command window or terminal.
<code>storageredir</code>	The <code>storageredir</code> command performs all storage redirection operations.

TABLE 60 Storage Redirection Command Options

Option Name	Description
<code>-h</code>	The <code>-h</code> command option displays the command-line Help information.
<code>-v</code>	The <code>-v</code> command option displays the Java command version information.

TABLE 61 Storage Redirection Sub-Commands

Sub-Command Name	Description
<code>list</code>	The <code>list</code> sub-command provides a list of the currently active storage redirections on one or all remote SPs. Syntax usage example: <code>storageredir list [-p storageredir_port] [remote_SP]</code>
<code>start</code>	The <code>start</code> sub-command invokes the specified redirection between the local host and the remote host server. If the authentication password is not provided, the system will prompt for it. Syntax usage example: <code>storageredir start -r redir_type -t redir_type_path -u remote_username [-s remote_user_password] [-p storageredir_port] remote_SP</code> Note - You must specify a valid admin (a) or console (c) role account in Oracle ILOM to start the redirection of storage device on a remote server.
<code>stop</code>	The <code>stop</code> sub-command stops the specified redirection between the local host and the remote host server. If the authentication password is not provided, the system will prompt for it. Syntax usage example: <code>storageredir stop -r redir_type -u remote_username [-s remote_user_password] [-p storageredir_port] remote_SP</code> Note - You must specify a valid admin (a) or console (c) role account in Oracle ILOM to stop the redirection of a storage device on a remote server.
<code>test-service</code>	The <code>test-service</code> sub-command verifies whether the Storage Redirection service connection is active on the local host. Syntax usage example: <code>storageredir test-service [-p storageredir_port]</code>

Sub-Command Name	Description
stop-service	The stop-service sub-command stops the Storage Redirection service connection to the remote host server. Syntax usage example: storageredir stop-service [-p storageredir_port]

TABLE 62 Storage Redirection Sub-Command Options

Sub-Command Option Name	Description
-r <i>redir_type</i>	The -r <i>redir_type</i> identifies the type of storage media being redirected. Valid device values for <i>redir_type</i> include: ■ CD-ROM device Syntax: -r cdrom ■ CD-ROM image: Syntax: -r cdrom_img ■ Floppy device: Syntax: -r floppy ■ Floppy image: Syntax: -r floppy_img
-t <i>redir_type_path</i>	The -t <i>redir_type_path</i> identifies the full path to where the storage redirection media is stored or mounted. Syntax usage example: -t /home/username/JRC_Test_Images/CDROM.iso
-u <i>remote_username</i>	The -u <i>remote_username</i> identifies the user name required to log in to the Oracle ILOM SP. Syntax usage example: -u john_smith Note - Any valid user account in Oracle ILOM can install or launch the Storage Redirection service or client on a local system. However, a valid admin (a) or console (c) role in Oracle ILOM is required to start or stop the redirection of a storage device on a remote server.
-s <i>remote_user_password</i>	The -s <i>remote_user_password</i> identifies the password required to log in to the Oracle ILOM SP. Syntax usage example: -s my_password If this password sub-command is not specified at the command line, the system will automatically prompt you for it.
-s <i>yes/no</i>	The -s <i>yes/no</i> option instructs the storage redirection service to accept the server security certificate in the case that the certificate is not trusted by the storage redirection service. If this option is not specified, in the case that the certificate is not trusted, the system will automatically prompt you for it.

Sub-Command Option Name	Description
	As of Oracle Firmware 3.2.5.3, the <code>-s yes/no</code> option applies when issuing the Start and Stop sub-commands. Syntax usage examples: -s yes or -s no
<code>-p storageredir_port</code>	The <code>-p storageredir_port</code> identifies the storage redirection communication port on the local host. The default port provided is 2121. Syntax usage example: -p 2121

Using the Oracle ILOM Remote System Console Plus

Note - The Oracle ILOM Remote System Console Plus is available on all newly released Oracle systems that shipped with Oracle ILOM firmware 3.2.1 or later.

Description	Links
Refer to these sections for information about the Oracle ILOM Remote System Console Plus features, as well as instructions for first time set up.	■ “Oracle ILOM Remote System Console Plus” on page 198 ■ “Remote System Console Plus First-Time Setup” on page 199
Refer to these sections for instructions on how to modify the KVMS Maximum Session count; or, to secure the host server operating system desktop upon exiting a redirection session.	■ “Modify KVMS Maximum Client Session Count (Optional)” on page 204 ■ “Set a Lock Mode to Secure the Host Server Desktop (Optional)” on page 205
Refer to these sections for information about launching and using the Oracle ILOM Remote System Console Plus client.	■ “Launching and Using the Oracle ILOM Remote System Console Plus” on page 207 ■ “Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards” on page 212 ■ “Toggle Button, Virtual Keys, and Status Icons” on page 215 ■ “Resolving Warning Messages for Self-Signed SSL Certificate ” on page 216 ■ “Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate” on page 218

Related Information

- *Oracle ILOM Security Guide (3.2.x)*, Using Remote KVMS Securely
- [“Using the Oracle ILOM Remote System Console Plus” on page 197](#)

Oracle ILOM Remote System Console Plus

Note - SPARC M8 series servers, as of firmware release 4.0.1.x do not support Oracle ILOM Plus. SPARC M8 Series servers support the Oracle ILOM Remote System VNC Console. For more details, see [“Connecting to the Oracle ILOM Remote System VNC Console” on page 163.](#)

The Oracle Integrated Lights Out Manager (ILOM) Remote System Console Plus is available on most newly released Oracle systems shipping with Oracle ILOM firmware 3.2.1 or later. The Oracle ILOM Remote System Console Plus includes both a text-based serial console and a graphic-based video console that enable system administrators to remotely redirect host server system keyboard, video, mouse, and storage devices.

The Oracle ILOM Remote System Console Plus supports the following serial and video redirection options:

- **Serial Line Redirection Session** (Oracle SPARC servers only) – The serial-line redirection option supports one full-control text-based console session for the primary user; and, one or more view-only text-based console sessions for all other signed-in users per server SP.

Maximum Number of Serial-Line Redirection Sessions

A maximum of one full-control serial-line redirection session can be launched from the Oracle ILOM Redirection web page. Additional text-based console sessions can be launch from the Oracle ILOM CLI (start /HOST/Console).

Note - Solaris users must use the serial-redirection mode in Oracle ILOM Remote System Console Plus to access the Solaris Host Console, view Solaris Host Console messages, or to issue Solaris Host Console commands such as boot commands. The video mode redirection option in the Oracle ILOM Remote System Console Plus must not be used to access the Solaris Host Console, view Solaris Host Console messages, or to issue Solaris Host Console commands such as boot commands.

- **Video Redirection Sessions** (Oracle x86 and SPARC servers) – The video redirection option supports one full-control graphic console session for the primary user; and, one or more view-only graphic console sessions for all other signed-in users per server SP.

Maximum Number of Video Redirection Sessions

By default, up to four video redirection sessions can be launched from the Oracle ILOM Remote System Control > Redirection web page. In addition, as of firmware release 3.2.4, a KVMS Maximum Client Session Count property is available for configuration. Use that property to limit the number of users who can view the video redirection session. To modify the Maximum Client Session Count property, see [“Modify KVMS Maximum Client Session Count \(Optional\)” on page 204.](#)

Note - Newer SPARC servers (S7-2 and later) support serial redirection mode only.

Redirection Privileges Granted to Remote System Console Sessions

Full-control redirection privileges are automatically enabled for a primary video or serial-line user. A primary user is the user who first starts a redirection session to the host server.

View-only redirection privileges are automatically enabled for users who establish a redirection session to the host server after a primary user has initiated a redirection session.

A primary user can relinquish full-control of the redirection session by exiting the video or serial session window, or by selecting Relinquish Full-Control in the KVMS menu of the video session window. A view-only user can take full-control of a relinquished full-control redirection session by exiting and relaunching the session window, or by selecting Take Full-Control from the KVMS menu in the video session window.

For further instructions for using the Oracle ILOM Remote System Console Plus client, see these topics:

- [“Remote System Console Plus First-Time Setup ” on page 199](#)
- [“Set a Lock Mode to Secure the Host Server Desktop \(Optional\)” on page 205](#)
- [“Launching and Using the Oracle ILOM Remote System Console Plus” on page 207](#)
- [“Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards” on page 212](#)

Note - The Oracle ILOM Remote System Console Plus does not support a CLI storage redirection client.

Note - If your system was shipped with an earlier firmware version than 3.2.1; or, if you upgraded your system from Oracle ILOM 3.0.x to 3.1.x or later, see [“Using the Oracle ILOM Remote System Console or Storage Redirection CLI” on page 167](#).

Remote System Console Plus First-Time Setup

To set up the Oracle ILOM Remote System Console Plus for first-time use, see these topics:

- [“Requirements for Using the Oracle ILOM Remote System Console Plus” on page 200](#)
- [“Configure Local Client KVMS Settings” on page 202](#)
- [“Modify KVMS Maximum Client Session Count \(Optional\)” on page 204](#)

- [“Set a Lock Mode to Secure the Host Server Desktop \(Optional\)” on page 205](#)

Requirements for Using the Oracle ILOM Remote System Console Plus

The following requirements must be met prior to using the Oracle ILOM Remote System Console Plus for the first time:

- [Table 63, “Requirements for Using Oracle ILOM Remote System Console Plus,” on page 200](#)

TABLE 63 Requirements for Using Oracle ILOM Remote System Console Plus

Set-Up Requirement	Description
Firmware	The Oracle ILOM Remote System Console Plus is available on most Oracle servers that shipped with Oracle ILOM 3.2.1 or later. Note - Newer SPARC servers (S7-2 and later) support serial redirection mode only in the Oracle Remote System Console Plus. To redirect the host server keyboard, video, and mouse (KVM) events to a graphical shared desktop display on newer SPARC servers, see “Connecting to the Oracle ILOM Remote System VNC Console” on page 163. Note - SPARC M8 series servers do not support the Oracle ILOM Remote System Console Plus. SPARC M8 series servers support the Oracle ILOM Remote System VNC Console only. For more details, see “Connecting to the Oracle ILOM Remote System VNC Console” on page 163
KVMS Settings	Configure SP local client properties for keyboard, mouse, and video redirection behavior. KVMS Defaults: KVMS State: Enabled, Mouse Mode: Absolute, Lock Mode: Disabled Related Information: ■ “Configure Local Client KVMS Settings” on page 202 ■ “Set a Lock Mode to Secure the Host Server Desktop (Optional)” on page 205 Note - Absolute Mouse Mode is recommended for all host server operating systems, with the exception of a Linux-based operating system that does not include mouse driver support for Absolute mode. In this case, for Linux-based systems without driver support, Relative Mouse Mode should be configured. As of Oracle ILOM firmware version 3.2.2, the Mouse Mode property in Oracle ILOM is configurable.
Hardware Mouse Pointer Settings for Oracle Solaris 11 and Linux Operating Systems Using Relative Mouse Mode	To gain better control of the mouse pointer when Relative Mouse mode is in use, the default hardware mouse settings for Acceleration, Sensitivity, and Threshold should be modified by following these steps: Step 1: Gain better control of the mouse: (Oracle Solaris and Linux OS) 1. Start a redirection session to the host server. For details see, “Launching and Using the Oracle ILOM Remote System Console Plus” on page 207. 2. Log in to the host server desktop and launch a terminal window. 3. In the terminal window, type: xset m 1 1 and press Enter. 4. Click Mouse Sync in the Oracle ILOM Remote System Console Plus redirection window.

Set-Up Requirement	Description
	Step 2: Make the mouse settings permanent: (Oracle Solaris and Linux OS) 1. On the host OS system, click System > Preferences > Mouse. 2. In the General tab of the Mouse dialog box, set the slowest parameter for Acceleration, the lowest parameter for Sensitivity, and the smallest parameter for threshold. Related Information: ■ Bandwidth and Low Bandwidth Usage Considerations in “Preference Menu Options” on page 214
Hardware Mouse Pointer Settings for Windows Operating Systems Using Relative Mouse Mode	To gain better control of the mouse pointer when Relative Mouse mode is in use on a Windows-based operating system, disable the Mouse Hardware option for Enhanced Pointer Precision by following these steps: 1. Click the Start > Control Panel > Mouse. 2. In the Mouse Properties dialog box, click the Pointer Options tab. 3. In the Pointer Options tab, disable the option for Enhanced Pointer Precision and click OK.
Java Runtime Environment	The Oracle ILOM Remote System Console Plus requires the Java Runtime Environment to be either Java 7 update 131 or later, Java 8, or Java 9. To download the latest Java Runtime Environment, go to http://java.com. Note - All Java versions support TLS v1.2. However, if a version <i>prior</i> to Java 7u131 is installed, you will need to manually enable TLS v1.2, or update your system with a later Java version. For information about configuring TLS properties in Oracle ILOM, see Table 38, “Web Server Configuration Properties,” on page 101.
Required JDK	■ For IPv4 networks, a 32-bit or 64-bit JDK is required. ■ For IPv6 networks, a 32-bit or 64-bit JDK170b36 or higher is required.
User Roles and Host Server User Credentials	■ The Admin (a) role is required in Oracle ILOM to modify the KVMS service State. ■ The Console (c) role is required in Oracle ILOM to modify KVMS properties (excluding the service State property) and to launch the Oracle ILOM Remote System Console Plus. ■ Host server user credentials are required to access the redirected host server operating system desktop.
Web Browser Support	For a list of supported web browsers, see “Supported Web Browsers for Oracle ILOM” on page 40 .
Video Redirection and Serial Redirection Use	When launching the Oracle ILOM Remote System Console Plus, users can launch a remote KVMS session using one of the following redirection methods: ■ Serial Redirection (Oracle SPARC servers only) – This option is only available for Oracle SPARC server SPs. When it is enabled, the serial-line redirection option supports a full-control text-based console session for the primary user and a view-only text-based console session for all other serial-line users that are currently signed in to the server SP. ■ Video Redirection – This option is available for Oracle x86 server SPs and SPARC server SPs. When it is enabled, the video redirection option supports a full-control GUI console session for the primary user and a view-only GUI console session for other signed-in users for each server SP.
Maximum Redirection Sessions	■ Maximum Serial-Line Redirection Sessions – A maximum of one serial-line redirection session, per SP, can be launched from the Oracle ILOM Redirection page.. ■ Video Redirection – By default, a maximum of four video redirection sessions, per SP, can be launched from the Oracle ILOM Redirection page. However, to prevent other signed-in video session users on the SP from viewing confidential data during a video session, you can set the Maximum Client Session Count property to 1. For instructions on how to modify the maximum number of video sessions launched from an SP, see “Modify KVMS Maximum Client Session Count (Optional)” on page 204.
Communication TCP/IP Ports Required	The Oracle ILOM Remote System Console Plus uses the following TCP/IP communication ports by default:

Set-Up Requirement	Description
	■ Port: 5120 for non-SSL encrypted storage media redirection ■ Port: 5555 for SSL encrypted storage media, video, and user authentication redirection For a complete list of default network ports, see “Default Network Ports Used by Oracle ILOM” on page 99.
Keyboard Support	See “International Keyboard Support” on page 215 .
Trusted SSL Certificate Support	As of Oracle ILOM firmware version 3.2.8, additional certificate checks will occur if the self-signed Default SSL Certificate is in use. For further information about these certificate checks, see: “Resolving Warning Messages for Self-Signed SSL Certificate ” on page 216. As of Oracle ILOM firmware 3.2.10, additional custom certificate checks will occur if the custom SSL certificate and private key are not properly configured. For instance: ■ A custom Certification Authority (CA) SSL Certificate and a Private Key are upload to Oracle ILOM. ■ The Java Keystore on the client side is not properly configured with the required root CA certificate to validate the uploaded custom SSL certificate and private key in Oracle ILOM. For further information about resolving warning messages for Custom SSL Certificates, see “Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate” on page 218.

▼ Configure Local Client KVMS Settings

Note - SPARC M8 series servers as of Oracle ILOM firmware 4.0.1.x do not support KVMS settings.

Before You Begin

- Administrator (a) role privileges must be enabled in Oracle ILOM to modify the KVM State property.
- Console (c) role privileges must be enabled in Oracle ILOM to modify the Host Lock Settings.
- The property for Mouse Mode is configurable in Oracle ILOM as of firmware release 3.2.2 or later.

Note - For servers running Oracle ILOM firmware version 3.2.1, Oracle ILOM automatically sets the applicable mouse mode based on the host server's hardware configuration.

1. To access the server SP KVMS settings in Oracle ILOM, do the following:

- **Web** – Click Remote Console > KVMS > KVMS Settings.
- **CLI** – Type:

```
show /SP/services/kvms
```

2. Modify the following KVMS properties as required:

Property	Default	Description
State (servicestate=)	Enabled	The KVMS service State is enabled by default for redirection. This State property must be enabled for you to use the Oracle ILOM Remote System Console Plus. If you disable the State property, you will not be able to use the Oracle ILOM Remote System Console Plus. CLI Syntax for KVMS Service State: set /SP/services/kvms servicestate=enabled disabled
Maximum Session Count (max_session_count=)	4	4 (default) 3 2 1 The Maximum Session Count property enables you to control the number of users permitted to view video redirection sessions that are launched from the server SP. The Maximum Session Count property is available in Oracle ILOM as of firmware release 3.2.4. For further configuration details, see “Modify KVMS Maximum Client Session Count (Optional)” on page 204.
Mouse Mode (mousemode=)	Absolute	Absolute Relative As of Oracle ILOM firmware version 3.2.2, the Mouse Mode property in Oracle ILOM is set to Absolute by default. Absolute mode is recommended for all host servers running Windows, Oracle Solaris, or a version of Linux that includes a driver that supports Absolute Mouse Mode. Use Relative Mouse Mode if the remote host is running a version of Linux that does not include a mouse driver that supports Absolute Mouse Mode. Note - If the mouse mode is modified when a primary user has a remote system console session opened on the SP, the change does not take affect until the primary session user either: 1) uses the KVMS menu in the session window to Relinquish Full-Control of the session and to Take Full-Control of the session; or, 2) exits and relaunches the session window. Taking these actions to change the mouse mode on the client, will cause any active storage redirection session on the SP to stop. CLI Syntax for Mouse Mode set /SP/services/kvms mousemode=absolute relative
Host Lock Mode (lockmode=)	Disabled	For details on how to set the host lock properties, see “Set a Lock Mode to Secure the Host Server Desktop (Optional)” on page 205.

3. To apply your modifications, click Save on the KVMS Settings page.

▼ Modify KVMS Maximum Client Session Count (Optional)

Oracle ILOM, by default, permits you to launch up to four video client sessions on an SP from the Remote Redirection web page. Optionally, you can limit the number of video client sessions on an SP by modifying the KVMS Maximum Client Session Count property in the CLI or web interface. For further details, see the following information.

Before You Begin

- Console (c) role privileges must be enabled in Oracle ILOM to modify the KVMS Maximum Client Session Count property.
- To prevent other signed-in video session users on the SP from viewing confidential information entered by a primary video session user, the Maximum Client Session Count property value must be set to 1.
- Upon resetting the Maximum Client Session Count property in Oracle ILOM, all active Oracle ILOM Remote System Console Plus video sessions on the SP will be terminated.

1. **To modify the Maximum Client Session Count property, follow the instructions below for the preferred Oracle ILOM interface.**

Oracle ILOM Interface	Instructions
Web	1. Navigate to the Remote Console > KVMS page. 2. In the KVMS page, modify the Maximum Client Session Count property value. Note - The minimum client video session value is 1. The default maximum client video session value is 4. 3. Click Save. A warning message appears to inform you that changing the Maximum Client Session Count property will cause all active remote console video sessions on the SP to terminate. 4. Click Yes to proceed; or, click No to cancel the operation.
CLI	1. Type: <pre>set /SP/services/kvms max_session_count=[1 2 3 4(default)]</pre> A warning message appears to inform you that changing the Maximum Client Session Count property will cause all active remote console video sessions on the SP to terminate. 2. Type "y" to proceed; or, type "n" to cancel the operation.

2. **After modifying the Maximum Client Session Count, relaunch the Oracle ILOM Remote Console Plus from the Remote Control > Redirection web page.**

For further details, see [“Launch and Use the Oracle ILOM Remote System Console Plus” on page 208](#).

Set a Lock Mode to Secure the Host Server Desktop (Optional)

Oracle ILOM provides the option to lock the host server desktop whenever a remote KVMS session disconnects. This feature ensures that if a KVMS session user closes the session prior to logging out of the host server desktop, subsequent KVMS session users will be prompted to enter their user credentials to gain access to the system.

For a description of lock mode options, as well instructions for configuring the lock mode in Oracle ILOM, see these topics:

- [Table 64, “Configurable Host Server Lock Options ,” on page 205](#)
- [“Lock Host Desktop When Disconnecting a Remote KVMS Session” on page 206](#)

TABLE 64 Configurable Host Server Lock Options

Lock Mode Property Setting	Description
Windows (lockmode=windows)	The Windows Lock Mode setting is configurable for host servers running a Microsoft Windows operating system. When the host Lock Mode property is set to Windows, Oracle ILOM works in conjunction with the standard Windows keyboard shortcut (Ctrl+Alt+Del K) for locking the Windows operating system desktop.
Custom (lockmode=custom)	The Custom Lock Mode setting is configurable for host servers running an Oracle Solaris operating system, a Linux-based operating system, or a Microsoft Windows operating system without using the Ctrl+Alt+Del K key sequence. When the host Lock Mode property in Oracle ILOM is set to Custom, Oracle ILOM supports the use of the following key sequences to lock the desktop: ■ A custom key sequence supported by Oracle Solaris or a Linux-based operating system. The custom key sequence needs to be defined on the host operating system prior to enabling the Custom Lock Mode setting in Oracle ILOM. For instructions for creating a custom key sequence, refer to the operating system vendor documentation. ■ A custom key sequence supported by Windows such as the Windows Logo Key+L keyboard shortcut. The Custom Lock Mode setting in Oracle ILOM does not support the standard Windows keyboard shortcut for locking the desktop (Ctrl+Alt+Del K).
Disabled (lockmode=disabled)	When the host Lock Mode property is set to Disabled (default), Oracle ILOM will not automatically lock the host server desktop when a remote KVMS session ends.

▼ Lock Host Desktop When Disconnecting a Remote KVMS Session

Before You Begin

- For Custom Lock Mode configurations, the custom key sequence must be defined on the host server operating system prior to setting the Custom Lock Mode option in Oracle ILOM.
- The Console (c) role is required to modify the host lock properties in Oracle ILOM.

1. Set a value for the host Lock Mode property in Oracle ILOM by doing the following:

- **Web – Click Remote Control > KVMS.** In the KVMS Settings page, click the Lock Mode list box to select one of the following values: Windows, Custom, or Disable.

- **CLI – Type:**

```
set /SP/services/kvms lockmode=windows|custom|disabled
```

If you set the Lock Mode property to Custom, proceed to Step 2. If you did not set the Lock Mode property to Custom and you are using the web interface, proceed to Step 3. Otherwise, you have completed the procedure.

2. If the Lock Mode property in Step 1 was set to Custom, perform the following to specify Custom Lock Modifiers and a Custom Lock Key:

- **Web – In the KVMS Settings page do the following:**

- a. Click the Custom Lock Modifiers list box and select the custom key sequence defined on the host server OS.
- b. Click the Custom Lock Key list box and select a custom lock key.

- **CLI – Type:**

- a. `set /SP/services/kvms lockmodifiers=value`

- b. `set /SP/services/kvms custom_lock_key=value`

Possible Custom Lock Modifiers Values: l_alt, r_alt, l_shift, r_shift, l_ctrl, r_ctrl, l_gui, r_gui

Up to four lock modifiers values can be specified. Each modifier can be separated by a comma.

Possible Custom Lock Key Values: esc, end, tab, ins, del, home, enter, space, break, backspace, pg_up, pg_down, scr_lck, sys_rq, num_plus, num_minus, f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, a-z, 0-9, !, @, #, \$, %, ^, &, *, (,), -, _ =, +, ?, |, ~, [, {, }, :, ;, <, >, /

See the Host Lock Configuration Example following this procedure.

3. To apply the property changes you made in the KVMS Settings page, click Save.

Host Lock Configuration Example:

If Shift+Control+Backspace was defined on the host server operating system as a custom lock key sequence, then the following KVMS lock properties would be set in the Oracle ILOM SP:

```
/SP/services/kvms
Properties:

  custom_lock_key = backspace
  custom_lock_modifiers = l_shift, l_ctrl
  lockmode = custom
  servicestate = enabled
```

Launching and Using the Oracle ILOM Remote System Console Plus

Note - SPARC M8 series servers as of firmware 4.0.1.x do not support Oracle ILOM Remote System Console Plus or KVMS configuration properties. SPARC M8 series servers support the Oracle ILOM Remote System VNC Console. For further details, see [“Connecting to the Oracle ILOM Remote System VNC Console” on page 163](#)

For instructions for launching and using the web-based Oracle ILOM Remote System Console Plus, see these topics:

- [“Launch and Use the Oracle ILOM Remote System Console Plus” on page 208](#)
- [“Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards” on page 212](#)
- [“Toggle Button, Virtual Keys, and Status Icons ” on page 215](#)

▼ Launch and Use the Oracle ILOM Remote System Console Plus

Before You Begin

- Ensure that the requirements for first-time use have been met: [Table 63, “Requirements for Using Oracle ILOM Remote System Console Plus,” on page 200.](#)
- Storage drive devices (such as CD, DVD, floppy, and USB devices) are automatically detected and listed in the Oracle ILOM Remote System Console Plus Storage Device dialog box. If bootable media is not detected in the drive, a lock icon will appear on the drive that is listed in the Storage Device dialog box.
- Storage images must be added to the Oracle ILOM Remote System Console Plus Storage Device dialog box after launching a KVM session.
- Solaris users must use the serial-redirection mode in Oracle ILOM Remote System Console Plus to access the Solaris Host Console, view Solaris Host Console messages, or to issue Solaris Host Console commands such as boot commands. The video mode redirection option in the Oracle ILOM Remote System Console Plus must not be used to access the Solaris Host Console, view Solaris Host Console messages, or to issue Solaris Host Console commands such as boot commands.
- The following user credentials are required:
 - Console (c) user role privileges are required to use the Oracle ILOM Remote System Console Plus.
 - To exclusively control storage media from the Oracle ILOM Remote System Console Plus application, you must have either:
 - Root privileges on the Linux client.
 - Administrator privileges on the Windows client.
 - “Run as Administrator” privileges upon starting the Java web start program that launches the Oracle ILOM Remote System Console Plus application.
 - A user account on the host server is required to log in to the redirected host desktop.

1. To launch the Oracle ILOM Remote System Console Plus, do the following:

- a. In the Oracle ILOM web interface, click **Remote Control > Redirection.**

Note - Alternatively, you can launch the Oracle ILOM Remote System Console Plus from the Actions panel on the Summary page.

- b. In the **Launch Redirection** page, select a redirection option (video or serial), and then click **Launch Redirection Console.**

Note - Full-control mode is automatically enabled for the primary user. View-only mode is automatically enabled for all subsequent signed-in session users.

After clicking the Launch Redirection Console button, the Oracle ILOM Remote System Console Plus window for video redirection shows the redirected host server desktop in its present state. For example:

- If the host server is powering on, a set of boot messages appear.
- If the host server operating system is powered-on, a GUI (graphical user interface) screen of the host desktop appears.
- If the host server is not powered-on, a snapshot of the last host console state prior to the power-off appears. For example, if the host login screen appeared prior to powering-off the server, the host login screen will appear in the KVMS session window. In this case, the server is actually powered-off and host redirection is disabled until the server is powered-on.

Note - If Oracle ILOM firmware 3.2.8 or later is installed and a Warning message (Check Certificate or Video Redirection Error) appears prior to launching the Oracle ILOM Remote System Console Plus, see [“Resolving Warning Messages for Self-Signed SSL Certificate”](#) on page 216.

2. To take full-control or relinquish full-control of the current redirection session, click either Take Full-Control or Relinquish Full-Control in the KVMS menu.

- **Take Full-Control** – A view-only user can choose to take full-control of the redirection session and force the existing primary user to view-only mode.
- **Relinquish Full-Control** – The primary user can relinquish full-control privileges for the current redirection session and switch to view-only mode.

Note - SPARC SP serial-line users. When full-control is applied to a serial-line redirection session in the KVMS window, all concurrent user CLI host console sessions (`/HOST/console`) will be forced to view-only mode. To gain full-control (read-write mode) in the CLI host console, the following must occur: 1) the primary KVMS user must relinquish full-control for serial-line redirection in the KVMS session window, and 2) the host console user must restart the CLI console session (`start -f /HOST/console`).

Note - SPARC or X86 SP video session users. By default, up to four video client sessions can be launched from the Oracle ILOM Redirection web page. To limit the maximum number of video sessions permitted on an SP, see [“Modify KVMS Maximum Client Session Count \(Optional\)” on page 204](#).

3. To redirect storage media, perform the following actions:

- a. Verify you have full-control privileges for the redirection session. If not, click Take Full-Control in the KVMS menu.**

Note - If you are the primary user with full-control privileges, the option for Take Full-Control is disabled in the KVMS menu.

- b. Click Storage in the KVMS menu.**

The Storage Device dialog box appears.

Note - The Storage Device dialog box automatically displays storage drive devices (such as CD, DVD, floppy, and USB devices) detected on the Oracle ILOM Remote System Console Plus client. If bootable media is not detected in the drive, a lock icon appears on the drive to indicate: 1) the drive is present, and 2) bootable media was not found in the drive.

- c. To add a storage image (such as a DVD image) to the Storage Device dialog box, click Add.**

- d. To redirect storage media from the Storage Device dialog box, select the storage media and click Connect.**

Note - To establish a redirection connection to a storage device, the Oracle ILOM Remote System Console Plus application must have exclusive control to the storage device. If the Oracle ILOM Remote System Console Plus does not have exclusive access to the storage device, the following error message appears: *Unable to open drive exclusively*. To resolve this error, you must ensure that the storage device is not being accessed, used, or probed by any other process or application on the client.

Note - After establishing a connection to the device, the label on the Connect button in the Storage Device dialog box will change to Disconnect.

- e. To stop a storage media redirection from the Storage Device dialog box, select the media, click Disconnect, and then click OK to close the dialog box.
 - f. To remove storage media from the Storage Device dialog box, click the storage media, and then click Remove.
 - g. To view a list of special considerations when redirecting storage media from the Storage Device dialog box, see Storage Media Considerations or USB Media Considerations in the [“KVMS Menu Options” on page 212](#)
4. To use the virtual keyboard, click Keyboard in the KVMS menu.
- For further information about the virtual keyboard menu option, see [“KVMS Menu Options” on page 212](#).

Note - You must have full-control privileges to use the virtual keyboard.

5. To change the power state of the local monitor on the managed server, click Turn Local Monitor On or click Turn Local Monitor Off in the KVMS menu.
- For further information about the local monitor menu options, see [“KVMS Menu Options” on page 212](#).

Note - You must have full-control privileges to power on or power off the local monitor on or off.

6. To exit the Oracle ILOM Remote System Console Plus, click Exit in the KVMS menu.

Related Information

- [“Requirements for Using the Oracle ILOM Remote System Console Plus” on page 200](#)
- [“Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards” on page 212](#)
- [“Set a Lock Mode to Secure the Host Server Desktop \(Optional\)” on page 205](#)

Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards

Refer to these topics for descriptions of Oracle ILOM Remote System Console Plus menu options and toggle key usage.

- [“KVMS Menu Options” on page 212](#)
- [“Preference Menu Options” on page 214](#)
- [“Help Menu Options” on page 215](#)
- [“International Keyboard Support” on page 215](#)

KVMS Menu Options

Menu Option	Description
Storage	The Storage option when selected opens the Storage Device dialog box. Storage Media Usage Considerations ■ The Oracle ILOM Remote System Console Plus application must be able to control the media device exclusively. No other process or application on the client can access, use, or probe the media device. If another process or application is using the media device while attempting to redirect the media device, the following message appears: <i>Unable to open the drive exclusively</i>. In this case, you must wait until the other process is done before you can attempt to redirect the storage device. ■ Supported storage media includes: physical optical drives (CD/DVD), physical floppy drives, and ISO images, which include single-session DVD ISO. In addition, USB floppy drives and USB memory sticks are supported. ■ Physical (or ISO) CDs or DVDs can be as large as the media permits (up to 600 MB for CD, 4.7 GB for DVD). The maximum floppy disk capacity can be as large as 1.44 MB. ■ Successful redirection of auto-detected storage devices requires that: 1) bootable media is present in the device; and 2) Administrator (Windows) or root (Linux) privileges on the host client are enabled to exclusively control the redirected storage device. ■ Storage media cannot be physically ejected during redirection. To change the redirected media, you must disconnect the redirected device prior to establishing another storage redirection in the Storage Device dialog box. ■ For Linux clients, multiple ISO images will not auto-mount on the host operating system. For these cases, the ISO images must be manually mounted upon starting the redirection and then manually unmounted upon stopping the redirection. ■ When you change a floppy disk, you should wait at least 5 seconds after ejecting the floppy to insert the new floppy; otherwise, the contents of the ejected floppy appear instead of the contents of the newly inserted floppy. ■ If you are installing software from distribution media (for example, a CD or DVD), ensure that the media is inserted in the local client redirected drive. ■ If you are installing software from an ISO DVD image, ensure that the ISO DVD image is stored on the local client or on a shared network file system.

Menu Option	Description
	USB Media Usage Considerations ■ When redirecting an 8 GB NTFS memory stick on a RHEL 4.8 32-bit client, the client system might take some time to detect and load the 8 GB NTFS memory stick. ■ The Oracle ILOM Remote System Console Plus application must have full control to the USB device. No other process or application on the client can access, use, or probe the device while attempting to redirect the device. For example, active processes such as the McAfee Endpoint process running on a Windows 7 client, or the Hardware Access Layer Daemon (HALD) process running on an Oracle Solaris client could prevent the Oracle ILOM Remote System Console Plus from gaining exclusive access to the storage device. If this occurs, you will likely need to disable (stop) the other process to permit the Oracle ILOM Remote System Console Plus exclusive access to the device. ■ Windows client users must login in as Administrator to gain full-control of a local USB device. ■ Prior to using the Storage Device dialog box on an SLES11SP1 client, you should use the command line to mount a USB memory stick, or to remove the mount point for a USB memory stick. ■ When redirecting a USB memory stick from a Linux client, the USB memory stick is not a supported bootable device.
Virtual Keyboard	The Virtual Keyboard option opens a Virtual Keyboard dialog box. By default, the language for the virtual keyboard is English. You can change the language in the Preference menu (see “Preference Menu Options” on page 214). Virtual Keyboard Usage Consideration ■ The Lock key, when enabled, will enable these special keys: shift, alt, ctrl, context, and windows. To release the special keys, disable the Lock key.
Turn Local Monitor On -or- Turn Local Monitor Off	The Turn Local Monitor On and Turn Local Monitor Off options control the display of the local monitor that is attached to the server. By default, the local monitor option is enabled (or turned on).
Take Full-Control -or- Relinquish Full-Control	The following options enable multiple users to switch between full-control mode and view-only mode: ■ Take Full-Control – When enabled, this option enables a view-only user to take full-control over the remote keyboard, mouse, and, if applicable, the remote storage media. If there is another primary user connected, the other primary user is forced to view-only mode. ■ Relinquish Full-Control – When enabled, this option enables the primary user to switch from full-control mode to view-only mode. Note - If full-control is either relinquished or taken away while redirecting storage media, the active storage redirection session will automatically be disconnected, as well as the session control for the keyboard and mouse.
Exit	The Exit option closes the Oracle ILOM Remote System Console Plus session.

Preference Menu Options

Preference Menu Option	Description
Mouse Sync on Mode Change (enabled by default)	Mouse Sync on Mode Change is enabled by default. When enabled (that is, when the check box is selected), the remote mouse and local mouse will automatically sync upon switching between full-control mode and view-only mode.
Language	English is the default language for the virtual keyboard. You can change the language of the virtual keyboard by 1) choosing another language from the Language list box, and 2) clicking OK. Note - The Language option on both the host server operating system and the Oracle ILOM Remote System Console Plus (Preference menu) must match.
Bandwidth	Unlimited is the default Bandwidth setting. You can change the Bandwidth setting by 1) choosing another option from the Bandwidth list box, and 2) clicking OK. Note - The Bandwidth option affects the data transfer rate between the local server and the Oracle ILOM Remote System Console Plus client. Bandwidth and Low Bandwidth Usage Considerations ■ Lowering the Bandwidth and the Low Bandwidth rate impacts both the video redirection quality and the mouse movement. ■ If a Matrox driver is detected on the host server, and if the Bandwidth default value is changed, there is no need to change the Low Bandwidth default value. ■ If a Matrox graphic driver is not detected on the host server, and if the Bandwidth rate is changed to any value other than Unlimited, the default value for Low Bandwidth must be changed to either 3 bpp (bits per pixel) or 8 bpp to resolve any problems with the mouse movement.
Low Bandwidth	Note: The Low Bandwidth Preference menu option is available in graphic mode only. 16 bpp is the default Low Bandwidth setting. You can modify the Low Bandwidth setting by 1) choosing another option from the Low Bandwidth list box, and 2) clicking OK.
Global Logging	Console and Log File is the default Global Logging setting. When this default option is enabled, event messages are printed directly to the Java Console and the Console Log File. You can modify the Global Logging target by 1) choosing another option from the Global Logging list box, and 2) clicking OK. Note - Choosing None will disable event logging for the Oracle ILOM Remote System Console Plus.
Logging Level	Error is the default Logging Level setting. The Error Logging Level represents only the highest level of reported errors and generates the fewest event messages in the log file. The Debug Logging Level captures all events and generates the most event messages in the log file. You can modify the Logging Level option by 1) choosing another option from the Logging Level list box, and 2) clicking OK.
Console Log File	The Console Log File is saved to your home directory by default.

Preference Menu Option	Description
	Click the Browse button to change the location for saving the log file, and then click OK in the Preference dialog box.

Help Menu Options

Help Menu Option	Description
Performance	The Performance option in the Help menu displays the last 10 video redirection frames per second.
About	The About option on the Help menu displays the current Java version and copyright date for the Oracle ILOM Remote System Console Plus client.

International Keyboard Support

The Oracle ILOM Remote System Console Plus supports the use of the following international keyboard language layouts:

■ Danish (Danish)	■ French (FR)	■ Japan (JP) Note: Only in English Mode.	■ Turkish - F (TR)
■ Dutch (NL)	■ French Belgium (FR)	■ Norwegian (NO)	■ Turkish - Q (TR)
■ Dutch Belgium (NL)	■ German (DE)	■ Portuguese (PT)	■ United Kingdom (EN)
■ English (US)	■ German (Swiss)	■ Spanish (ES)	
■ Finnish (FI)	■ Italian (IT)	■ Swedish (SV)	

Toggle Button, Virtual Keys, and Status Icons

Refer to the following table for descriptions of the Oracle ILOM Remote System Console Plus toggle buttons, virtual keys, and status icons.

Item	Description
Mouse Sync Button	The Mouse Sync button appearing on the Oracle ILOM Remote System Console Plus client window enables you to manually sync the local and remote mouse pointers. Note - When taking full KVMs control, it is not necessary to sync the mouse pointers.
Virtual Keys	The following virtual keys appear on the Oracle ILOM Remote System Console Plus client window. These virtual keys provide the same behavior during a KVMs session as the keys found on your keyboard. ■ L Ctl – Control key on left side of spacebar

Item	Description
	■ L Win – Window key on left side of spacebar ■ L Alt – Alt key on left side of spacebar ■ R Alt – Alt key on right side of spacebar ■ R Win – Window key on right side of spacebar ■ R Ctl – Control key on right side of spacebar ■ Context – Menu key on keyboard ■ Lock – Caps Lock key on keyboard ■ Ctrl+Alt+Del – Control key, Alt key, and Delete key pressed on keyboard
Status Icons	The following redirection status icons appear on Oracle ILOM Remote System Console Plus client window: ■ Keyboard and mouse combination icon – Shows keyboard redirection status: a highlighted icon – ON, a grey icon – OFF, and a red icon – Error ■ Storage icon – Shows storage redirection status: a highlighted icon – ON, a grey icon – OFF, and a red icon – Error ■ Monitor icon – Shows monitor redirection status: a highlighted icon – ON, and a grey icon – OFF
Lock icon on storage drive device	Storage drives on the Oracle ILOM Remote System Console Plus client are automatically detected and listed in the Storage Device dialog box. If bootable media is not detected in the drive, a lock icon will appear on the drive listed in the Storage Device dialog box.

Resolving Warning Messages for Self-Signed SSL Certificate

Note - The following information applies to the users of the Oracle ILOM Remote System Console and the Oracle ILOM Remote System Console Plus.

As of Oracle ILOM firmware version 3.2.8, unless a custom signed SSL certificate is in use, additional certificate checks will be conducted by Oracle ILOM when the self-signed Default SSL Certificate is in use.

Note - For further information about using a trusted SSL certificate in Oracle ILOM, see [“Improve Security by Using a Trusted SSL Certificate and Private Key” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x.](#)

When the Default SSL Certificate is in use, Oracle ILOM remote KVMS console users might experience one of the following warning messages:

- **Certificate Check Warning Message** — The security certificate of this server is untrusted.
Required user action: Follow these steps to ensure the Default SSL certificate is valid:
 1. Take note of the host certificate fingerprint value appearing on the Warning dialog box.

2. Access the SSL Certificate page in Oracle ILOM to confirm that the host certificate fingerprint value appearing on the Warning dialog box matches the host certificate fingerprint value listed on the SSL Certificate page.

Note - To access the SSL Certificate page, click ILOM Administration > Management Access > SSL Certificate.

3. Perform one of the following:

- If the host certificate fingerprint values match in Step 2, you can choose to: 1) bypass the Warning message by clicking the Continue (not recommended) button, or 2) exit launching the remote system console by clicking the Abort System Console button.

Note - Prior to clicking the Continue (not recommended) button you should consult with your security officer or system administrator for guidance on how to proceed.

- If the host certificate fingerprint values do not match in Step 2, you should click the Abort System Console button and follow-up with your security officer or system administrator for resolution.
 - **Video Redirection Error** — Man-in-the -middle attack is occurring or the self-signed Default SSL Certificate and fingerprint have changed.
 - **Required User Action** — Perform the following steps:
 1. Consult with your security office or system administrator to confirm that the Default SSL Certificate changed.
 2. After receiving confirmation that the Default SSL Certificate changed, you can choose to either remove the host certificate fingerprint file from the local user directory or edit the local host certificate fingerprint file with the last fingerprint value issued by Oracle.
 - To remove the host certificate fingerprint file, select the local host certificate fingerprint file (ilomrc_known_hosts or jrc2_known_hosts) in the local user directory (/user|home/username) and click Delete. Upon removing the stale fingerprint file in the local user directory, relaunch the remote system console and refer to the steps for resolving the Certificate Check warning message.
- or-
- To edit the host certificate fingerprint file with the last fingerprint value issued by Oracle, follow these steps:
 - a. Using a text editor open the fingerprint file (ilomrc_known_hosts or jrc2_known_hosts) in the local user directory (/user|home/username)

- b. Remove the fingerprint value listed in the local host certificate fingerprint file .
- c. Open the Oracle ILOM web interface and copy the fingerprint value appearing on the SSL Certificate page and paste it in to the local host certificate fingerprint file.

Ensure that the spacing between the IP address and the fingerprint value is preserved.
- d. Save the changes to the local host certificate fingerprint file and relaunch the remote system console.

Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate

Note - The following information applies to the users of the Oracle ILOM Remote System Console and the Oracle ILOM Remote System Console Plus.

As of Oracle ILOM firmware version 3.2.10, additional certificate checks will be conducted by Oracle ILOM when a custom SSL certificate is configured.

Note - For further information about using a trusted SSL certificate in Oracle ILOM, see [“Improve Security by Using a Trusted SSL Certificate and Private Key” in Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x.](#)

When the Custom CA SSL Certificate is in use, Oracle ILOM remote KVMS console users might experience a warning message. For instance:

- **Oracle ILOM Remote System Console Plus Users - Warning Message** — Remote host can not be identified: Could not validate the Remote Host Certificate. Either a man-in-the-middle attack could be occurring or it is possible that the remote host certificate has been changed.
- **Oracle ILOM Remote System Console Users - Warning Message** — Certification validation failed. Could not validate the Remote Host Certificate. Either a man-in-the-middle attack could be occurring or it is possible that the remote host certificate has been changed.

A warning message occurs when the Java client is not properly configured to validate a custom CA SSL certificate that is currently being used by Oracle ILOM. The Java client uses a keystore to validate CA certificates. In cases where the required root CA certificate or intermediate root CA certificate is not in the Java keystore, the validation will fail.

Required User Action: Follow these steps to ensure the custom CA SSL Certificate can be validated.

1. Verify that the required root CA certificate or intermediate root CA certificate is configured in client side Java keystore. To view the Java keystore, use the keytool command with the `-list` option, for example:

- On a Windows system, at the prompt, type:

```
keytool -list -keystore "c:\Program Files (x86)\Java\jre<version>\lib\security\cacerts"
```

- On a Linux system, at the prompt, type:

```
keytool -list -keystore $JAVA_HOME/jre/lib/security/cacerts
```

2. Locate the alias and/or fingerprint of the root CA certificate or intermediate root CA certificate that is required by the custom CA certificate currently configured in Oracle ILOM.

If the required root CA Certificate or intermediate root CA certificate is missing in the Java keystore, consult with your security officer or system administrator prior to continuing this procedure to add the missing CA certificate details to the Java keystore.

3. Use the `-importcert` keytool command to add the missing root CA certificate or intermediate root CA certificate to the Java keystore. For example:

- On a Windows system, at the prompt, type:

Note - The `-importcert` command needs to be run as an administrator. To start a command prompt as an administrator on a Windows system: Click Start, click All Programs, and then click Accessories. Right-click Command prompt, and then click Run as administrator.

```
keytool -importcert -alias certalias -file root-ca-cert -keystore "c:\Program Files (x86)\Java\jre<version>\lib\security\cacerts"
```

- On a Linux system, at the prompt, type:

```
keytool -importcert -alias certalias -file root-ca-cert -keystore $JAVA_HOME/jre/lib/security/cacerts
```

4. Verify that the required root CA certificate or intermediate root CA certificate is now available in the Java keystore using the keytool command with the `-list` and `-alias` options, for example:

- On a Windows system, at the prompt, type:

```
keytool -list -alias certalias -keystore "c:\Program Files (x86)\Java\jre<version>\lib\security\cacerts"
```

- On a Linux system, at the prompt, type:

```
keytool -list -alias certalias -keystore $JAVA_HOME/jre/lib/security/cacerts
```

Configuring Host Server Management Actions

Description	Links
Refer to this section for descriptions of CMM and SP configurable properties for host power control.	■ “Controlling Host Power to Server or Blade System Chassis ” on page 222
Refer to this section for descriptions of SP configurable diagnostic properties.	■ “Setting Diagnostic Tests to Run” on page 223
Refer to this section for descriptions of x86 SP configurable properties for next boot device.	■ “Setting Next Boot Device on x86 Host Server” on page 230
Refer to this section for descriptions of SPARC SP properties for host control.	■ “Setting Host Control and Boot Properties on SPARC Host Server” on page 233
Refer to this section for descriptions of SPARC SP configurable boot mode properties for OpenBoot and LDoms.	■ “Overriding SPARC Host Boot Mode” on page 238
Refer to this section for instructions on how to set Verified Boot properties	■ “Configuring SPARC Verified Boot Properties” on page 240
Refer to this section for descriptions of SPARC SP configurable boot properties for host domain, as well as a list of LDom configurations currently set.	■ “Managing SPARC Host Domains” on page 242
Refer to this section for descriptions of SPARC SP configurable property values for the host KeySwitch state.	■ “Setting SPARC Host KeySwitch State ” on page 244
Refer to this section for descriptions of SPARC SP configurable property values for the host TPM state.	■ “Setting SPARC Host TPM State ” on page 245
Refer to this section for descriptions of SPARC SP configurable property values for host state capture on error.	■ “Setting SPARC Host State Capture” on page 248
Refer to this section for descriptions of SPARC host I/O reconfiguration property values.	■ “Managing SPARC Host I/O Reconfiguration Policy” on page 250
Refer to this section for instructions for viewing host assignments for PDomains and DCUs, as well as managing SPM and SPP failover behavior.	■ “Managing SPARC PDomains and DCU Assignments” on page 251
Refer to this section for instructions on how to redirect host output to rear VGA port.	■ “Redirecting Host Output to Rear VGA Port ” on page 259

Related Information

- [“Maintaining x86 BIOS Configuration Parameters” on page 317](#)

Controlling Host Power to Server or Blade System Chassis

Oracle ILOM provides a set of parameters that enables system administrators to control the power state of a host server or a blade chassis system.

System administrators can issue power control commands from the Oracle ILOM CLI or web interface. For more details about each power control command, see the following table.

Note - For Oracle multi-domain server systems, you can control the power state on individual server domains.

TABLE 65 Remote Power Control Commands for Host Managed Devices

User Interface Configurable Target and User Role:			
■ CLI: <code>[command] /System</code> (or for multi-domain servers: <code>[command] /Servers/PDomains/PDomain_n/HOST</code>) ■ Web: Host Management > Power Control ■ User Role: Admin (a) role			
Requirement:			
■ To apply a selected power option in the web interface, you must click Save.			
Web	CLI	Applies to:	Description
Reset	■ x86 SP: <code>reset /System</code> ■ SPARC: <code>reset - force /System</code>	■ Any managed server	Use Reset to assert a power-cycle to a managed server, while keeping power applied to system components (such as disk drives and so).
Graceful Reset	■ <code>reset /System</code>	■ SPARC managed server only	Use Graceful Reset to gracefully shut down the host operating system prior to power-cycling the managed server.
Immediate Power Off	■ <code>stop -force /System</code>	■ Any managed server or blade system chassis	Use Immediate Power Off to directly shut down the power to the managed device.
Graceful Shutdown and Power Off	■ <code>stop /System</code>	■ Any managed server or blade system chassis	Use Graceful Shutdown and Power Off to gracefully shut down the host operating system prior to shutting down the power to the managed device.
Power On	■ <code>start /System</code>	■ Any managed server or blade system chassis	Use Power On to apply full power to the managed device.
Power Cycle	■ <code>stop /System</code> ■ <code>start /System</code>	■ Any managed server	Use Power Cycle to turn off system power to all system components and then apply full power to all system components.

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Setting Diagnostic Tests to Run

Oracle ILOM provides a set of server-specific diagnostic properties that enable system administrators to control whether system diagnostic tests are run at startup. These diagnostic properties are configurable from either the Oracle ILOM CLI or web interface. For further information about these properties, see the following tables:

- [Table 66, “x86 Server SP Diagnostic Properties ,” on page 223](#) x86 Server SP Diagnostics Properties
- [Table 67, “Legacy SPARC Systems Host Diagnostic Properties \(M6, M5, T5, and earlier\),” on page 224](#) Legacy SPARC Systems Host Diagnostic Properties (M6, M5, T5 and earlier)
- [Table 68, “Newer SPARC Systems Host Diagnostic Properties \(M7, T7, and later\),” on page 226](#) Newer SPARC Systems Host Diagnostic Properties (M7, T7 and later)
- [Table 69, “Newer SPARC Systems SP Diagnostic Properties \(M7, T7, and later\),” on page 229](#) Newer SPARC Systems SP Diagnostic Properties (M7, T7 and later)

TABLE 66 x86 Server SP Diagnostic Properties

User Interface Configurable Target and User Role:		
■ SP CLI: /HOST ■ Web: Host Management > Diagnostics ■ User Role: Reset and Host Control (r) role (required to modify diagnostic properties).		
Requirement:		
■ To apply diagnostic property modifications in the web interface, you must click Save.		
Property	Default	Description
Run Diagnostics on Boot (diag state= <i>disabled</i> <i>enabled</i> <i>extended</i> <i>manual</i>)	Disabled	<i>Disabled</i> <i>Enabled</i> <i>Extended</i> <i>Manual</i> ■ Disabled – The PC-Check diagnostic tests are not run upon powering on the x86 server. ■ Enabled – The basic PC-Check diagnostic tests are run upon powering on the x86 server, which take approximately 3 minutes to complete. ■ Extended – The extended PC-Check diagnostic tests are run upon powering on the x86 server, which take approximately 20 minutes to complete. ■ Manual – The PC-Check diagnostic tests are run in manual mode upon resetting the power on the server. The PC-Check diagnostic test menu appears upon powering on the server enabling you to manually activate the tests.

User Interface Configurable Target and User Role:

- SP CLI: /HOST
- Web: Host Management > Diagnostics
- User Role: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click Save.

Property	Default	Description
CLI Syntax for Diagnostics on Boot State:		
set /HOST/diag state=disabled enabled extended>manual		
Generate NMI button (generate_host_nmi=true)	No value	This option, when enabled, sends a non-maskable interrupt to the host operating system. Note - Depending on the host operating system configuration this action might cause the operating system to either: crash, stop responding, or wait for external debugger input. CLI Syntax to Generate NMI: set /HOST/ generate_host_nmi=true

TABLE 67 Legacy SPARC Systems Host Diagnostic Properties (M6, M5, T5, and earlier)**User Interface Configurable Target and User Role:**

- SP CLI: /HOST/diag (or, /Servers/PDomains/PDomain_n/Host/diag)
- Web: Host Management > Diagnostics
- User Role: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click Save.

Property	Default	Description
Trigger (trigger=error-reset hw-change power-on-resets)	HW-Change	<i>Power-On HW-Change Error-Reset</i> Specify one or more of the following triggers to cause a Power-On-Self-Test (POST) to run. ■ Power On – When enabled, a Power-On-Self-Test (POST) is run upon powering on the SPARC server. ■ HW-Change – When enabled, a Power-On-Self-Test (POST) is run at startup when the following hardware changes occur: FRU replacement, cover removal, or AC power cycle. ■ Error-reset – When enabled, a Power-On-Self Test (POST) is run after any error-invoked power reset occurs. CLI Syntax for Trigger: For SPARC single-server SP, type: set /HOST/diag trigger=error-reset hw-change power-on-resets

User Interface Configurable Target and User Role:

- SP CLI: /HOST/diag (or, /Servers/PDomains/PDomain_n/Host/diag)
- Web: Host Management > Diagnostics
- User Role: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click **Save**.

Property	Default	Description
		For SPARC multi-domain server SP, type: set /Servers/PDomains/PDomain_n/HOST/ diag trigger=error-reset hw-change power-on-resets
Trigger Levels (power_on_level= hw_change_level= error_reset_level=)	Max	Max Min Independently set a test level for each enabled trigger. ■ Max – When enabled, runs the maximum level of diagnostic tests. ■ Min – When enabled, runs the minimum level of diagnostic tests. CLI Syntax for Trigger Levels: For SPARC single-server SP, type set /HOST/diag error_reset_level=min max hw_change_level=min max power_on_level=min max For SPARC multi-domain server SP, type: set Servers/PDomains/PDomain_n/HOST/diag error_reset_level=min max hw_change_level=min max power_on_level=min max
Trigger Verbosity (power_on_verbosity= hw_change_verbosity= error_reset_verbosity=)	Min	Normal Min Max Debug None Independently set a report level for each enabled trigger: ■ Normal – When enabled, Oracle ILOM outputs a moderate amount of debugging information to the system console. Output includes the name and results for each test run. ■ Min – When enabled, Oracle ILOM outputs a limited amount of output on the system console (default). ■ Max – When enabled, Oracle ILOM outputs debugging information for each POST step to the system console. ■ Debug – When enabled, Oracle ILOM outputs an extensive debugging information to the system console. Output includes the names of the components tested and the test results for each test run. ■ None – When enabled, Oracle ILOM disables the output of debugging information to the system console. CLI Syntax for Trigger Verbosity:

User Interface Configurable Target and User Role:

- SP CLI: /HOST/diag (or, /Servers/PDomains/PDomain_n/Host/diag)
- Web: Host Management > Diagnostics
- User Role: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click Save.

Property	Default	Description
		set /HOST/diag/ error_reset_verbosity=normal min max debug none hw_change_verbosity=normal min max debug none power_on_verbosity=normal min max debug none
Mode (mode=)	Normal	<i>Off Normal</i> Set a mode to enable or disable the Power-On-Self Test for all enabled triggers. ■ Off – Prevents the Power-On-Self-Test (POST) to run for all enabled triggers. ■ Normal – Runs the Power-On-Self-Test (POST) for all enabled triggers. (default) CLI Syntax for Mode: set /HOST/diag/ mode=normal off

TABLE 68 Newer SPARC Systems Host Diagnostic Properties (M7, T7, and later)**User Interface Configurable Target and User Role:**

- SP CLI: /HOST/diag (or, /Servers/PDomains/PDomain_n/HOST/diag)
- Web: Host Management > Diagnostics
- User Role: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click Save.
- Oracle ILOM Firmware 3.2.5.5 and later.

Property	Default	Description
Default Level and Verbosity (default_level=)	Level = Off	Level: <i>Off Min Max</i>
(default_verbosity=)	Verbosity = Normal	Verbosity: <i>Normal None Min Max Debug</i>
		The default setting enables you to specify one of the following Power-On-Self-Test (POST) behaviors to occur upon a routine system power-on. ■ Level Off (default)– When enabled, POST will not run upon routine system power-on. - Level Min – When enabled, the POST will run basic diagnostic tests upon routine system power-on.

User Interface Configurable Target and User Role:

- SP CLI: `/HOST/diag` (or, `/Servers/PDomains/PDomain_n/HOST/diag`)
- Web: Host Management > Diagnostics
- User Role: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click **Save**.
- Oracle ILOM Firmware 3.2.5.5 and later.

Property	Default	Description
		Level Max – When enabled, the POST will run basic diagnostic tests and extensive processor and memory tests upon routine system power-on.
		■ Verbosity Normal – When enabled, a moderate amount of debugging output to system console. Output includes test name and results.
		Verbosity None – When enabled, no debugging output is printed to the system console.
		Verbosity Min – When enabled, a limited amount of debugging output is printed to the system console.
		Verbosity Max – When enabled, all the POST step debugging output is printed to system console.
		Verbosity Debug – (<i>The Debug setting is no longer supported as of Oracle ILOM firmware version 3.2.6 or SPARC SW 9.7.x.</i>) When enabled, an extensive amount of debugging output is printed to system console. Output includes the names of the devices being tested, as well as the results of each test.

CLI Syntax Default Level and Verbosity:

For a SPARC single-host server SP, type:

```
set /HOST/diag default_level=off|min|max default_verbosity=normal|
none|min|max
```

For a SPARC multi-domain server SP, type:

```
set /Servers/PDomains/PDomain_n/HOST/diag default_level=off|min|
max default_verbosity=normal|none|min|max
```

Error Reset Level and Verbosity (error_level=) (error_verbosity=)	Level = Max	Level: <i>Off Max Min</i>
	Verbosity = Normal	Verbosity: <i>Normal None Min Max</i>
		Independently set a test level for each enabled trigger.
		■ Level Max – When enabled, runs the maximum level of diagnostic tests upon an error invoked reset.
		Level Min – When enabled, runs the limited level of diagnostic tests upon an error invoked reset.
		Level Off – When Enabled, the POST will not run upon an error invoked reset.
		■ Verbosity Normal – When enabled, a moderate amount of debugging output to system console. Output includes test name and results.

User Interface Configurable Target and User Role:

- **SP CLI:** /HOST/diag (or, /Servers/PDomains/PDomain_n/HOST/diag)
- **Web:** Host Management > Diagnostics
- **User Role:** Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click **Save**.
- Oracle ILOM Firmware 3.2.5.5 and later.

Property	Default	Description
		Verbosity None – When enabled, no debugging output is printed to the system console. Verbosity Min – When enabled, a limited amount of debugging output is printed to the system console. Verbosity Max – When enabled, all the POST step debugging output is printed to system console. Verbosity Debug – When enabled, an extensive amount of debugging output is printed to system console. Output includes the names of the devices being tested, as well as the results of each test.
CLI Syntax for Error Rest Level and Verbosity: For SPARC single-host server SP, type <pre>set /HOST/diag error_reset_level=off min max verbosity_level=normal\none min max</pre> For SPARC multi-domain server SP, type: set Servers/PDomains/PDomain_n/HOST/diag error_reset_level=off min max verbosity_level=normal none min max debug		
HW_Change Level and Verbosity	Level = Max	Level: Off Min Max
(hw_change_level=)	Verbosity = Normal	Verbosity: None Min Max Debug
(hw_change_verbosity=)		■ Level Max – When enabled, the POST will run the maximum level of diagnostic tests in the event of a hardware change such as a power cycle, chassis cover removal, or FRU replacement. Level Min – When enabled, the POST will run a limited level of diagnostic tests in the event of a hardware change such as a power cycle, chassis cover removal, or FRU replacement. Level Off – When Enabled, the POST will not run a series of texts in the event of a hardware change such as a power cycle, chassis cover removal, or FRU replacement. ■ Verbosity Normal – When enabled, a moderate amount of debugging output to system console. Output includes test name and results. Verbosity None – When enabled, no debugging output is printed to the system console. Verbosity Min – When enabled, a limited amount of debugging output is printed to the system console.

User Interface Configurable Target and User Role:

- SP CLI: /HOST/diag (or, /Servers/PDomains/PDomain_n/HOST/diag)
- Web: Host Management > Diagnostics
- User Role: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click **Save**.
- Oracle ILOM Firmware 3.2.5.5 and later.

Property	Default	Description
		Verbosity Max – When enabled, all the POST step debugging output is printed to system console.
		Verbosity Debug – <i>(The Debug setting is no longer supported as of Oracle ILOM firmware version 3.2.6 or SPARC SW 9.7.x.)</i> When enabled, an extensive amount of debugging output is printed to system console. Output includes the names of the devices being tested, as well as the results of each test.
CLI Syntax for Trigger Verbosity:		
For SPARC single-host server SP, type		
set /HOST/diag/ hw_change_verbosity=normal min max debug none		
hw_change_level=off min max		
For SPARC multi-domain server SP, type:		
set /Servers/PDomains/PDomain_n/HOST/diag hw_change_level=off min max		
hw_change_verbosity=normal none min max debug		

TABLE 69 Newer SPARC Systems SP Diagnostic Properties (M7, T7, and later)**User Interface Configurable Target and User Role:**

- SP CLI: /SP/diag
- Web: System Management > Diagnostics
- User Role: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click **Save**.
- Oracle ILOM Firmware 3.2.5.5 and later.

Property	Default	Description
Default Level	Level = Off	Level: <i>Off Min Max</i>
(default_level=)		Specify the appropriate diagnostic behavior in the event of a routine server power cycle (power off/on) or a server reset. By default, the Default Level for POST is set to <i>Off</i> . Note - The POST Default Level property does not apply to error-invoked resets or hardware change events. ■ Off (default) — Select Off to prevent POST from running. ■ Min — Select Min to run a basic suite of diagnostic tests.

User Interface Configurable Target and User Role:

- SP CLI: `/SP/diag`
- Web: System Management > Diagnostics
- User Role: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click **Save**.
- Oracle ILOM Firmware 3.2.5.5 and later.

Property	Default	Description
		■ Max — Select Max to run a basic suite of diagnostic tests plus extensive processor and memory tests. CLI Syntax: set /SP/diag default_level=off min max
HW Change (hw_change_level=)	Level = Max	Level: <i>Max Min Off</i> Specify the appropriate diagnostic behavior in the event of a server power-cord-cycle, server top cover removal, or FRU (field-replaceable unit) replacement. By default, the HW Change Level for POST is set to Max. Note - A server power-cord-cycle refers to when the power cords are removed, replaced, or when the power is first applied to server. ■ Max (default) — Select Max to run a basic suite of diagnostic tests plus extensive processor and memory tests. ■ Min — Select Min to run a basic suite of diagnostic tests. ■ Off — Select Off to prevent POST from running. CLI Syntax: set /SP/diag hw_change_level=off min max

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Setting Next Boot Device on x86 Host Server

Oracle ILOM provides a set of x86 server properties that enables system administrators to set the next boot device on the host server. However, these configurable boot device properties in Oracle ILOM, apply only to the next time the x86 server powers on.

Note - After the system powers on and boots the Oracle ILOM user-specified boot device, the system reverts to the boot device properties set in the system BIOS Utility.

System administrators can set the x86 server property for the next boot device from the Oracle ILOM CLI or web interface. For more details about using the x86 system next boot device properties in Oracle ILOM, see the following table.

Note - For details about how to move devices in the boot order or to make persistent changes to the boot order using the BIOS Utility, see the BIOS section in the x86 server administration guide for selecting a boot device. For details about how to move devices in the boot order or to make persistent changes to the boot order using the Oracle Hardware Management Pack (HMP) software, see the `biosconfig` section in the *Oracle Server CLI Tools User's Guide*.

TABLE 70 Set Next Boot Device Property on x86 Managed Server

User Interface Configurable Target and User Role:	
■ SP CLI: <code>/HOST/boot_device=</code> ■ SP Web: Host Management > Host Control > Next Boot Device ■ User Role: Reset and Host Control (r) role	
Requirement:	
■ To apply a next boot device option in the web interface, you must click Save.	
Property Value	Description
Default (Use BIOS Settings) (<code>boot_device=default</code>)	Set the Default BIOS property to have the x86 system boot from the first device that is currently set in the system BIOS boot order. CLI Syntax: Single server: <pre>set /HOST/boot_device=default</pre> Multi-domain server: <pre>set /Servers/PDomains/PDomain_n/HOST/boot_device=default</pre>
PXE (<code>boot_device=pxe</code>)	Set the PXE property to temporarily bypass the system BIOS boot order at the next host boot and to boot the x86 system over the network using the PXE boot specification. CLI Syntax: Single server: <pre>set /HOST/boot_device=pxe</pre> Multi-domain server: <pre>set /Servers/PDomains/PDomain_n/HOST/boot_device=pxe</pre>

User Interface Configurable Target and User Role:

- SP CLI: /HOST/boot_device=
- SP Web: Host Management > Host Control > Next Boot Device
- User Role: Reset and Host Control (r) role

Requirement:

- To apply a next boot device option in the web interface, you must click Save.

Property Value	Description
Disk (boot_device=disk)	Set the Disk property to temporarily bypass the system BIOS boot order at the next host boot and to boot the first disk device as determined by the BIOS Utility boot order. Note - Use the Disk property to boot from either a fixed hard disk drive (HDD) or a removable HDD, such as a USB flash device. CLI Syntax: Single server: set /HOST/boot_device=disk Multi-domain server: set /Servers/PDomains/PDomain_n/HOST/boot_device=disk
Diagnostic (boot_device=diagnostic)	Set the Diagnostic property to temporarily bypass the system BIOS boot order at the next host boot and to boot the system from the diagnostic partition, if configured. CLI Syntax: Single server: set /HOST/boot_device=diagnostic Multi-domain server: set /Servers/PDomains/PDomain_n/HOST/boot_device=diagnostic
CDROM (boot_device=cdrom)	Set the CDROM property to temporarily bypass the system BIOS boot order at the next host boot and to boot the system from the attached CD-ROM or DVD device. CLI Syntax: Single server: set /HOST/boot_device=cdrom Multi-domain server: set /Servers/PDomains/PDomain_n/HOST/boot_device=cdrom
Floppy	Set the Floppy property to temporarily bypass the system BIOS boot order settings at the next host boot and to boot from the attached floppy device.

User Interface Configurable Target and User Role:

- SP CLI: /HOST/boot_device=
- SP Web: Host Management > Host Control > Next Boot Device
- User Role: Reset and Host Control (r) role

Requirement:

- To apply a next boot device option in the web interface, you must click Save.

Property Value	Description
(boot_device=floppy)	CLI Syntax: Single server: set /HOST/boot_device=floppy Multi-domain server: set /Servers/PDomains/PDomain_n/HOST/boot_device=floppy
BIOS (boot_device=bios)	Set the BIOS property to temporarily by-pass the BIOS boot order at the next host boot and to boot the system to the BIOS Utility Setup Menu. CLI Syntax: Single server: set /HOST/boot_device=bios Multi-domain server: set /Servers/PDomains/PDomain_n/HOST/boot_device=bios

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Setting Host Control and Boot Properties on SPARC Host Server

Oracle ILOM provides a set of SPARC server properties that enables system administrators to view host control information, as well as optionally set properties to control system boot behavior.

System administrators can view host control information or set configurable SPARC server boot properties from the Oracle ILOM CLI or web interface. For more details about these properties, see the following table.

Note - CLI paths for multi-domain SPARC servers are not provided in the following table. For these type of servers, append `/Servers/PDomains/PDomain_n` to the start of the CLI paths described in the following tables. For further information about performing these actions on a multi-domain SPARC server, refer to the administration guide for the server.

TABLE 71 Host Control Information and Boot Properties on SPARC Managed Server

User Interface Configurable Target and User Role:		
■ SP CLI: <code>/HOST property_name</code> ■ Web: Host Management > Host Control ■ User Role: Reset and Host Control (r) role is required to modify host configurable properties.		
Requirement:		
■ To apply property modifications made on the web Host Control page, you must click Save.		
Property	Default	Description
Host Control Information	Read-only properties	View SPARC server host control information for:
/HOST		■ MAC Address – Displays Ethernet MAC address assigned to managed device. ■ Hypervisor Version – Displays Hypervision firmware version. ■ OBP– Displays the OpenBoot PROM (OBP) firmware version. ■ POST Version – Displays the current POST version. ■ SysFW Version – Displays the current Oracle ILOM firmware version installed. ■ Host Status – Displays the current power state for the host operating system. CLI Syntax for Host Control Information: show /HOST
Alert Forwarding	Disabled	Disabled (default) Enabled
(alert_forwarding=)		The Alert Forwarding property controls whether the SP will forward events to the host system operating system (OS). Note - The Alert Forwarding property became configurable as of Oracle ILOM 4.0.1.x. Prior to the 4.0.1.x firmware release, the Alert Forwarding property was set to enabled by default and was not configurable. When set to disabled, the events are not forwarded to the host OS. When set to enabled, events are forwarded to the host OS and appear as "SC Alert: message" on the host OS console.

User Interface Configurable Target and User Role:

- SP CLI: `/HOST property_name`
- Web: Host Management > Host Control
- User Role: Reset and Host Control (r) role is required to modify host configurable properties.

Requirement:

- To apply property modifications made on the web Host Control page, you must click Save.

Property	Default	Description
CLI Syntax for Alert Forwarding		
set /HOST alert_forwarding disabled enabled		
<i>Reset Dump Core None</i>		
Auto Restart Policy (autorestart=)	Reset	Set to instruct the Oracle ILOM which action to take if the host operating system hangs. ■ Reset (default) – . Oracle ILOM attempts to reset the Oracle Solaris guest when the watchdog timer expires. ■ None – Oracle ILOM takes no action other than to issue a warning. ■ Dump Core – Oracle ILOM attempts to force a core dump of the operating system when the Oracle Solaris watchdog timer expires. CLI Syntax for Auto Restart Policy: set /HOST autorestart=reset dumpcore none
Hardware BTI Mitigation	Enabled	Default Enabled Disabled Note - The Hardware BTI Mitigation property is available for configuration as of Oracle ILOM firmware version 4.0.2.x on SPARC T5 servers, M-Series servers, or later SPARC platforms. Web interface: Note - To set the Hardware BTI Mitigation property on a SPARC M-Series server, navigate to the Host Management >Host Control page on the appropriate PDomain page . ■ Default – When Default is selected, the system will use the Oracle default setting for hardware-based mitigation for CVE-2017-5715 (Branch Target Injection, Spectre Variant 2). The Default property is enabled by default. ■ Enabled – Select Enabled to turn on the hardware-based mitigation mode for CVE-2017-5715 (Branch Target Injection, Spectre Variant 2), regardless of the Default property value. When enabled, this property provides a secure configuration option, but some applications might experience lower performance. ■ Disabled – Select Disabled to turn off the hardware-based mitigation mode for CVE-2017-5715 (Branch Target Injection, Spectre Variant 2), regardless of the Default property value. When disabled, the system might be

User Interface Configurable Target and User Role:

- SP CLI: `/HOST property_name`
- Web: Host Management > Host Control
- User Role: Reset and Host Control (r) role is required to modify host configurable properties.

Requirement:

- To apply property modifications made on the web Host Control page, you must click Save.

Property	Default	Description
		vulnerable to Branch Target Injection style attacks, but some applications might experience improved performance.
		CLI Syntax for Hardware BTI Mitigation:
		SPARC M-Series (PDomains):
		set /Servers/PDomains/PDomain_#/HOST hw_bti_mitigation= default disabled enabled
Auto Run on Error (autorunonerror=)	Poweroff	<i>None Powercycle Poweroff</i> Note - Powercycle is the default setting on SPARC M5 series servers and some M7 series servers. Action to be taken when the host encounters an error that requires a restart. ■ None - No action is taken if a fatal error is encountered. ■ Powercycle - The host is power cycled if a fatal error is encountered. ■ Poweroff (default) - The host is powered off if a fatal error is encountered. CLI Syntax for Auto Run on Error: set /HOST autorunonerror=none powercycle poweroff Note - For earlier Oracle SPARC servers, like the T-3 Series servers, the properties for autorunonerror=<i>true false</i>. When set to <i>true</i>, the host is power cycled if a fatal error is encountered. When set to <i>false</i> (default), the host is powered off if a fatal error is encountered.
Boot Timeout (boottimeout=)	0, timer disabled	0 (default) Integers 300 to 3600 Enter a time-out value for the boot timer in seconds. This value will be used if the host boot process fails. The boot timer is disabled by default (set to 0) CLI Syntax for Boot Timeout: set /HOST boottimeout= [0, 300... 360000]
Boot Restart Policy (bootrestart=)	None, policy disabled	<i>None Reset</i> Set to instruct Oracle ILOM whether to restart the SPARC server if the system times out.

User Interface Configurable Target and User Role:

- SP CLI: `/HOST property_name`
- Web: Host Management > Host Control
- User Role: Reset and Host Control (r) role is required to modify host configurable properties.

Requirement:

- To apply property modifications made on the web Host Control page, you must click Save.

Property	Default	Description
CLI Syntax for Boot Restart Policy:		
set /HOST bootrestart=reset none		
Max Boot Fails Allowed (maxbootfails=)	3 attempts	Integer between 0 and 10000 attempts. Set the maximum number of attempts allowed if the Oracle Solaris boot process fails. If the host does not boot successfully within the number of tries indicated by max boot fail, the host is powered off or power cycled (depending upon the setting of boot fail recovery). In either case, boot timeout is set to 0 (zero seconds), disabling further attempts to restart the host. CLI Syntax for Max Boot Fails Allowed: set /HOST maxbootfails=0 to 10000
Boot Fail Recovery (bootfailrecovery=)	Poweroff	Powercycle Poweroff None Set this property to instruct Oracle ILOM which action to take if the boot process is unsuccessful after reaching the maximum number of boot attempts. ■ Poweroff (default) – Oracle ILOM powers off the SPARC server after reaching the maximum boot attempts allowed. ■ Powercycle – Oracle ILOM power cycles the SPARC server after reaching the maximum boot attempts allowed. ■ None - The Boot Fail Recovery property is disabled. CLI Syntax for Boot Fail Recovery: set /HOST bootfailrecovery=off none powercycle

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Overriding SPARC Host Boot Mode

Oracle ILOM provides a set of host boot mode properties that enables system administrators to override the default method for booting the host operating system on the SPARC server.

The host boot mode properties in Oracle ILOM are intended to help resolve corrupt boot mode settings with OpenBoot or LDOMs. The boot mode properties, when set in Oracle ILOM, apply only to a single boot and expire within 10 minutes if the power on the host SPARC server is not reset.

System administrators can use the Oracle ILOM CLI or web interface to set the host boot mode properties. For more details about these properties, see the following table.

TABLE 72 Host Boot Mode Properties for Host SPARC Server

User Interface Configurable Target and User Role:		
■ SP CLI: <code>/HOST/bootmode</code> (or for multi-domain host servers: <code>/Servers/PDomains/PDomain_n/Host/bootmode</code>) ■ SP Web: Host Management > Host Boot Mode ■ User Role: Reset and Host Control (r) role (required to modify host boot mode configurable properties).		
Requirement:		
■ To apply boot mode property changes in the Host Boot Mode Settings page, you must click Save.		
Property	Default	Description
State (state=)	Normal	<i>Normal Reset NVRAM</i> Set to instruct Oracle ILOM to which action to take when the power on the SPARC server is reset. ■ Normal – Oracle ILOM preserves the current NVRAM variable properties. ■ Reset NVRAM – Oracle ILOM returns all OpenBoot variables to default property values upon the next SPARC server power reset. CLI Syntax to Set Host Boot Mode State: ■ For single-server SP, type: <code>set /HOST/bootmode state=normal reset_nvram</code> ■ For multi-domain server SP, type: <code>set /Servers/PDomains/PDomain_n/HOST/bootmode state=normal reset_nvram</code>
Expiration Date (expires=)	No value, read-only property	Bootmode properties expire within 10 minutes or when the power on the SPARC server resets (which ever comes first). The LDOM Config and Script properties do not expire and are cleared upon the next server reset or when the values are manually cleared.

User Interface Configurable Target and User Role:

- SP CLI: /HOST/bootmode (or for multi-domain host servers: /Servers/PDomains/PDomain_n/Host/bootmode)
- SP Web: Host Management > Host Boot Mode
- User Role: Reset and Host Control (r) role (required to modify host boot mode configurable properties).

Requirement:

- To apply boot mode property changes in the Host Boot Mode Settings page, you must click Save.

Property	Default	Description
CLI Syntax to View Host Boot Mode Expiration Date:		
■ For single-server SP, type: show /HOST/bootmode expires ■ For multi-domain server SP, type: show /Servers/PDomains/PDomain_n/HOST/bootmode expires		
Script		Up to 1000 bytes in length.
(script=)		The script controls the host SPARC server OpenBoot PROM firmware method for booting. The script is read when: (1) the State is set to Reset NVRAM, (2) power on the SPARC server is reset, and (3) OpenBoot variables are reset to defaults. Note - Service personnel might instruct you to specify a script for problem resolution. The full extent of script capabilities is not documented and exist primarily for debugging. CLI Syntax to Set Host Boot Mode Script: set /HOST/bootmode script=value Where: script does not affect the current /HOST/bootmode setting. value can be up to 1000 bytes in length. You can specify a /HOST/bootmode setting and specify the script within the same command. For example: set /HOST/bootmode state=reset_nvram script="setenv diag-switch? true"
LDOM Config	Factory-default	<i>Factory-default Valid LDOM Config</i>
(config=)		Instruct Oracle ILOM which LDOM configuration to use upon resetting the power on host SPARC server: ■ Factory-default – The factory-default configuration is the initial configuration where the platform appears as a single system hosting only one operating system. Use the factory-default configuration in Oracle ILOM to regain access to all system resources (CPUs, memory, I/

User Interface Configurable Target and User Role:		
■ SP CLI: /HOST/bootmode (or for multi-domain host servers: /Servers/PDomains/PDomain_n/Host/bootmode) ■ SP Web: Host Management > Host Boot Mode ■ User Role: Reset and Host Control (r) role (required to modify host boot mode configurable properties).		
Requirement:		
■ To apply boot mode property changes in the Host Boot Mode Settings page, you must click Save.		
Property	Default	Description
		O) that might have been assigned to other domains. The Factory-default property value might be necessary if you removed the Logical Domains Manager before restoring factory defaults using the Logical Domains OS software. ■ Valid LDOM Config – Enter the name of a valid active logical domain configuration.
CLI Syntax for Host Boot Mode LDOM Config:		
<pre>set /HOST/bootmode config={factory-default valid_LDOM_configuration}</pre>		

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Configuring SPARC Verified Boot Properties

On some of Oracle's SPARC systems, Verified Boot can be used to verify system boot blocks and Oracle Solaris kernel modules before they are loaded on the system. Use Oracle ILOM to enable Verified Boot and to specify how the system should respond when a verification check fails. Enabling Verified Boot can prevent harmful changes to the system boot blocks or Oracle Solaris kernel modules from taking effect. For further details about setting this policy in Oracle ILOM, see the property descriptions in [Table 73, “Verified Boot Properties,” on page 241](#).

To use the Verified Boot feature, Oracle Solaris 11.2 or later must be installed on the system.

Before you upload certificates to verify Oracle Solaris kernel modules, ensure that the following requirements are met:

- The certificates can be accessed through your network or local file system.
- The certificates are in PEM format, following the X.509 standard.

- The certificates are *not* encrypted with a passphrase.

TABLE 73 Verified Boot Properties

User Interface Configurable Target and User Role:		
■ SP CLI: <code>/Host/verified_boot</code> (or, <code>/Servers/PDomains/PDomain_n/Host/verified_boot</code>) ■ Web: Host Management > Verified Boot ■ User Role: Reset and Host Control (r) role		
Property	Default	Description
Boot Policy (<code>boot_policy</code>)	none	<i>none warning enforce</i> ■ none – The system does not run verification checks on boot blocks, unix, or geunix. ■ warning – When a verification check fails, a warning message is logged on the host console, and the boot process continues. ■ When a verification check fails, an error message is logged on the host console, and the boot process is aborted. CLI Syntax for Boot Policy: Single host server: <pre>set /Host/verified_boot boot_policy=none warning enforce</pre> Multi-domain host server: <pre>set /Servers/PDomains/PDomain_n/HOST/verified_boot boot_policy=none warning enforce</pre> Note - When Boot Policy for Verified Boot is set to Enforce and the Non-volatile RAM configuration variable for "use-nvramrc?" is set to True, the Solaris boot operation might fail on some SPARC platforms (such as SPARC T7 and M7 series server). For further details, see the 3.2.5 Known Issues section in the <i>Oracle ILOM Feature Updates and Release Notes</i>.
System Certificates (<code>/system_certs/1</code>)		View the <code>system_certs/1</code> target for details about pre-installed certificate files, such as the issuer and subject of the file.
User Certificates (<code>/user_certs/n</code>)		Load up to five custom certificate files to verify Solaris kernel modules other than unix and geunix. View the <code>user_certs/n</code> target for details about user-loaded certificate files, such as the issuer and subject of the files. CLI Syntax to Load Custom Certificate at Boot: Single host server: <pre>set /Host/verified_boot/user_certs/n load_uri=protocol://certificate_URI</pre> Multi-domain host server:

User Interface Configurable Target and User Role:		
■ SP CLI: /Host/verified_boot (or, /Servers/PDomains/PDomain_n/Host/verified_boot)		
■ Web: Host Management > Verified Boot		
■ User Role: Reset and Host Control (r) role		
Property	Default	Description
		set /Servers/PDomains/PDomain_n/Host/verified_boot/user_certs/n load_uri=protocol://certificate_URI
		Where <i>n</i> is the ID you want to associate with the certificate file and protocol is any of the transfer protocols supported by Oracle ILOM. For a list of supported protocols, see “Supported File Transfer Methods” on page 50
		CLI Syntax to Remove Verified Boot Custom Certificate:
		Single host server:
		reset /Host/Verified_boot/user_certs/n
		Multi domain host server:
		reset /Servers/PDomains/PDomain_n/Host/verified_boot/user_certs/n
		Where <i>n</i> is the ID of the certificate file you want to remove.

Managing SPARC Host Domains

Oracle ILOM provides a set of host domain properties that enable system administrators to view logical domain configurations presently set on a host SPARC server, as well as set host domain properties for auto-boot and boot guests.

The Oracle ILOM host domain properties are viewable and configurable from the Oracle ILOM CLI and web interface. For more details about these properties, see the following tables:

- [Table 74, “View Logical Domain Configurations Detected for Host SPARC Server,” on page 243](#) View Logical Domain Configurations Detected for Host SPARC Server
- [Table 75, “Host Domain Configurable Properties for Host SPARC Server ,” on page 243](#) Host Domain Configurable Properties for Host SPARC Server

TABLE 74 View Logical Domain Configurations Detected for Host SPARC Server

User Interface Configurable Target:	
■ SP CLI: <code>/HOST/domain/configs</code> ■ Web: Host Management > Host Domain	
Requirements:	
■ Logical domain configurations must be created on host SPARC server operating system. For information on how to create logical domain configurations, see the Oracle VM Server for SPARC documentation. ■ To view logical domain configurations, issue the show command (<code>show /HOST/domain/configs</code>)	
Property	Description
Domain Configurations (read-only)	Oracle ILOM displays a list of logical domain configurations detected on the host operating system. Oracle saves the detected logical domain configurations in non-volatile memory and updates the listing as changes occur.

TABLE 75 Host Domain Configurable Properties for Host SPARC Server

User Interface Configurable Target:		
■ SP CLI: <code>/HOST/domain/control</code> ■ Web: Host Management > Host Domain ■ User Role: Reset and Host Control (r) role (required to modify host domain configurable properties).		
Requirements:		
■ Logical domain configurations must be created on host SPARC server operating system. For information on how to create logical domain configurations, see the Oracle VM Server for SPARC documentation. ■ To apply host domain property changes in the Host Domain Settings page, you must click Save.		
Property	Default	Description
Auto-Run	Enabled	<i>Enabled Disabled</i>
(auto-boot=)		When the property for Auto-Run is enabled, the OpenBoot setting for auto-boot is enforced after the next domain reset. When the property for Auto-Run is disabled, automatic booting is prevented and the host control domain will stop at the OpenBoot OK prompt upon the next domain reset. CLI Syntax for Host Domain Auto-Run: For single-server SP, type: <pre>set /HOST/domain/control auto-boot=enabled disabled</pre> For multi-domain server SP, type: <pre>set /Servers/PDomains/PDomain_n/HOST/domain/control auto-boot=enabled disabled</pre>
Boot Guests	Enabled	<i>Enabled Disabled</i>

User Interface Configurable Target:

- SP CLI: /HOST/domain/control
- Web: Host Management > Host Domain
- User Role: Reset and Host Control (r) role (required to modify host domain configurable properties).

Requirements:

- Logical domain configurations must be created on host SPARC server operating system. For information on how to create logical domain configurations, see the Oracle VM Server for SPARC documentation.
- To apply host domain property changes in the Host Domain Settings page, you must click Save.

Property	Default	Description
(boot_guests=)		When the property for Boot Guests is enabled, Oracle ILOM boots the guest domains at the next server power-on or reset. When the property for Boot Guests is disabled, the configured guest domains are prevented from booting upon the next server power-on or reset. Note - The boot_guests property automatically reverts to Enabled (default property) after the server resets. CLI Syntax for Host Domain Boot Guests: For single-server SP, type: <pre>set /HOST/domain/control boot_guests=enabled disabled</pre> For multi-domain server SP, type: <pre>set /Servers/PDomains/PDomain_n/HOST/domain/control boot_guests=enabled disabled</pre>

Setting SPARC Host KeySwitch State

Oracle ILOM provides a KeySwitch property that enables system administrators to set the KeySwitch state for the host SPARC server. The KeySwitch property is configurable from the Oracle ILOM CLI or web interface. For further details about the KeySwitch configurable property values, see the following table.

TABLE 76 KeySwitch State Property Values for Host SPARC Server

User Interface Configurable Target and User Role:		
■ SP CLI: /HOST ■ Web: Host Management > KeySwitch > KeySwitch ■ User Role: Admin (a) role (required to modify KeySwitch property).		
Requirement:		
■ To apply changes to the Keyswitch property in the web interface, you must click Save.		
Property	Default	Description
Keyswitch	Normal	<i>Normal Standby Diag Locked</i>
(keyswitch_state=)		■ Normal – The SPARC server can power itself on and start the boot process. ■ Standby – The SPARC server is prevented from powering on. ■ Diag – The SPARC server can power on and use the Oracle ILOM default host diagnostic property values to provide fault coverage. When enabled, this option overrides user-specified Oracle ILOM diagnostic property values. ■ Locked – The SPARC server can power itself on, however you are prohibited from updating flash devices or modify the CLI property value set for /HOST send_break_action=break.
CLI Syntax for KeySwitch:		
For single-server SP, type:		
set /HOST keyswitch_state=normal standby diag locked		
For multi-domain server SP, type:		
set /Servers/PDomains/PDomain_n/HOST keyswitch_state=normal standby diag locked		

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Setting SPARC Host TPM State

Oracle ILOM provides a set of Oracle Solaris TPM properties that enable system administrators to manage the state of the Trusted Platform Module (TPM) feature on the host SPARC server.

The TPM property is configurable from the Oracle ILOM CLI or web interface. For further details about TPM configurable property values, see the following tables.

Note - TPM properties for x86 servers are managed in the BIOS Utility. For further details about x86 operating system TPM properties and requirements, refer to the Oracle x86 server administration guide.

- [Table 77, “TPM Property Values for Host SPARC Servers ,” on page 246](#) TPM Property Values for Host SPARC Server
- [Table 78, “TPM Property Values for Legacy Host SPARC Servers,” on page 247](#) TPM Property Values for Legacy Host SPARC Servers

TABLE 77 TPM Property Values for Host SPARC Servers

User Interface Configurable Target and User Role:		
■ SP CLI: /HOST/tpm (or, /Servers/PDomains/PDomain_n/host/tpm) ■ Web: Host Management > TPM > TPM Settings ■ User Role: Reset and Host Control (r) role (required to modify TPM property).		
Requirements:		
■ The host SPARC server must be running an Oracle Solaris Operating System version that supports TPM. ■ To apply TPM property modifications in the web interface, you must click Save.		
Property	Default	Description
TPM (mode=) (forceclear=)	Disabled ('off')	<i>Mode = activated (enabled) deactivated (disabled) off (default); Forceclear= false (default) true</i> ■ Mode – Set one of the following: ■ Activated – Enables the TPM state on the SPARC server at the next host power-on event. Note - "Enabled" mode label appears on M8 and T8 Systems versus the "Activated" label. ■ Deactivated – Disables the TMP state on the SPARC server at the next host power-on event. Note - "Disabled" mode label appears on M8 and T8 Systems versus the "Deactivated" label. ■ Off – Ignores the TPM chip on the SPARC server. ■ Forceclear – To clear the TPM device data on the SPARC server at the next host power-on event, set the property for Forceclear to 'true' and set the property for Mode to 'Activated'. Note - The Forceclear property is automatically set to 'false' after the next host power-on event. CLI Syntax to Set TPM Properties: For a single-server SP, type:

User Interface Configurable Target and User Role:

- SP CLI: /HOST/tpm (or, /Servers/PDomains/PDomain_n/host/tpm)
- Web: Host Management > TPM > TPM Settings
- User Role: Reset and Host Control (r) role (required to modify TPM property).

Requirements:

- The host SPARC server must be running an Oracle Solaris Operating System version that supports TPM.
- To apply TPM property modifications in the web interface, you must click Save.

Property	Default	Description
		set /HOST/tpm mode=[off deactivated activated] forceclear=false true
		For a multi-domain server SP, type:
		set /Servers/PDomains/PDomain_n/HOST/tpm mode=[off deactivated activated] forceclear=false true

TABLE 78 TPM Property Values for Legacy Host SPARC Servers**User Interface Configurable Target and User Role:**

- SP CLI: /HOST/tpm
- Web: Host Management > TPM > TPM Settings
- User Role: Reset and Host Control (r) role (required to modify TPM property).

Requirements:

- The host SPARC server must be running an Oracle Solaris Operating System version that supports TPM.
- To apply TPM property modifications in the web interface, you must click Save.

Property	Default	Description
TPM	Disabled ('false')	Enable=false true; Forceclear=false true; Activate=false true
(enable=)		To enable the SPARC server TPM device on the next host power-on event, set the properties for Enable and Activate to 'true'.
(activate=)		To purge all TPM device data on the SPARC server, set the property for Enable to 'false' and set the property for Forceclear to 'true'.
(forceclear=)		Note - The Forceclear property is automatically set to 'false' after the next host power-on event.
		CLI Syntax to Set TPM Properties:
		For a single-server SP, type:
		set HOST/tpm enable=[true false] activate=[true false] forceclear=false true

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Setting SPARC Host State Capture

Oracle ILOM provides host state capture properties that enable system administrators to control the type of data captured if fatal errors occur. The captured data is stored in Oracle ILOM and is obtainable when a service snapshot is taken from Oracle ILOM. The host state capture properties are configurable from the Oracle ILOM CLI or web interface. For further details about the host state capture configurable property values, see the following table.

TABLE 79 Host State Capture Properties for SPARC Server

User Interface Configurable Target and User Role:		
■ SP CLI: <code>/Host/</code> (or, <code>/Servers/PDomains/PDomain_n/Host</code>) ■ Web: Host Management > Host Control ■ User Role: Admin (a) role (required to modify state capture properties)		
Property	Default	Description
State Capture on Error (<code>state_capture_on_error=</code>)	enabled	<i>enabled disabled</i> That State Capture on Error property controls whether or not Oracle ILOM collects host state data upon detecting a fatal error on the host SPARC server. CLI Syntax for State Capture on Error: For SPARC single-server SP, type: set /HOST state_capture_on_error=enabled disabled For SPARC multi-domain server SP, type: set /Servers/PDomains/PDomains_n/HOST state_capture_on_error=enabled disabled
State Capture Mode (<code>state_capture_mode=</code>)	default	<i>redstate_scandump fatal_scandump default</i> The State Capture Mode property determines the type of data collected when an error occurs. ■ default - When an error occurs, only error register data is collected and saved to Oracle ILOM. ■ fatal Scandump - (Note: This option is supported on M8 hosts only as of Oracle firmware version 4.0.1.x) When a Fatal Reset error occurs, error register and

User Interface Configurable Target and User Role:

- SP CLI: /Host/ (or, /Servers/PDomains/PDomain_n/Host)
- Web: Host Management > Host Control
- User Role: Admin (a) role (required to modify state capture properties)

Property	Default	Description
		scandump data is collected and saved to Oracle ILOM. For all other errors, only error register data is recorded.
		■ redstate Scandump - (Note: This option is supported on M8 hosts only as of as of Oracle firmware 4.0.1.x) When a Red State exception occurs, error register and scandump data is collected and saved to Oracle ILOM. For all other errors, only error register data is recorded.
CLI Syntax for State Capture Mode:		
For SPARC single-server SP, type:		
set /HOST state_capture_mode=fatal_scandump default redstate_scandump		
For SPARC multi-domain server SP, type:		
set /Servers/PDomains/PDomains_n/HOST state_capture_mode=fatal_scandump default redstate_scandump		
State Capture Status (state_capture_status)	read-only	The State Capture Status property displays the current host capture state. Possible status states include: ■ Enabled = The State Capture on Error feature is enabled. ■ Disabled = The State Capture on Error feature is disabled. ■ Debug = The State Capture on Error debug feature is enabled. Note: The debug feature can only be set in the Oracle ILOM CLI and is used to run additional diagnostics when a host fatal error is encountered. The resulting output is saved to Oracle ILOM and available as part of a service snapshot ■ fatal-in-progress = The host has encountered a fatal error and its current state is being captured ■ debug-fatal-in-progress = The host has encountered a fatal error and the debug script is running. This status appears only when the debug feature is enabled in the Oracle ILOM CLI. ■ None = There is no status available when the host is powered off.

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Managing SPARC Host I/O Reconfiguration Policy

For some SPARC servers, Oracle ILOM provides a policy that enables system administrators to control whether the host IO paths are optimized and require modification at the next power on or power reset. By default, the host I/O reconfigure policy is enabled and configurable from the Oracle ILOM CLI or web interface. For further details about setting this policy in Oracle ILOM, see the following table.

Note - Reconfiguring the I/O paths will change the PCIe addresses and external addresses associated with boot devices.

Note - If the PCIe switches in the I/O path are not currently in use, and ioreconfigure is set to true, configure the I/O paths for maximum connectivity. Otherwise, configure the new paths for optimal I/O bandwidth

TABLE 80 SPARC Host I/O Reconfiguration Policy Properties

User Interface Configurable Target and User Role:		
■ SP CLI: /Host (or /Servers/PDomains/PDomain_n/host) ■ SP Web: Host Management > Host Control ■ User Role: Reset Host Control (r) role (required to modify this property).		
Property	Default	Description
IO Reconfigure Policy	true	<i>false true add_only</i>
(ioreconfigure=)		■ true – When enabled, Oracle ILOM (if necessary) will check and reconfigure the I/O paths each time the server SP or PDomain is powered on or reset. Note: PCIe switches will be configured to create the minimum required number of virtual switches to connect all of the available root complexes, which might result in changes to the I/O paths. ■ false – When enabled, Oracle ILOM will not check and reconfigure the I/O paths each time the server SP or PDomain is powered on or reset. Note: As of Oracle ILOM firmware release 4.0.1.1, the IO Reconfigure Policy property is automatically set to false when the control domain creates its first guest domain, ■ add_only – When enabled and when a new CMP (root complex) has been added since the last boot or reset, Oracle ILOM will reconfigure the I/O paths for optimal bandwidth. Note: The add_only property value is only supported on Oracle SPARC T5, M5, and M6 platforms.
CLI Syntax for IO Reconfigure Policy		
For SPARC single-server SP, type:		

User Interface Configurable Target and User Role:

- SP CLI: /Host (or /Servers/PDomains/PDomain_n/host)
- SP Web: Host Management > Host Control
- User Role: Reset Host Control (r) role (required to modify this property).

Property	Default	Description
		<code>set /SP/Host ioreconfigure=true false add_only</code>
		For SPARC multi-domain server SP, type:
		<code>set /Servers/PDomains/PDomain_n/Host ioreconfigure=true false add_only</code>

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Managing SPARC PDomains and DCU Assignments

On some SPARC servers such as M5, M6, and M7 series servers, Oracle ILOM provides properties for managing Host-DCU assignments and PDomain-DCU assignments.. For further details, see the following sections:

- [“Host-DCU Assignments and DCU-SPP Failover Behavior” on page 251](#)
- [“PDomain and DCU Assignments” on page 255](#)

Host-DCU Assignments and DCU-SPP Failover Behavior

For SPARC servers, like the M series servers, you can use Oracle ILOM to identify the host-DCU assignments, as well as to determine the general health of logical DCU configurations. In addition, for SPARC servers, like the M7-16 servers, which support a DCU service processor proxy (SPP) configuration with redundant service processor modules (SPM), you can use Oracle ILOM to determine the SPM that is actively assigned to manage the DCU system activity. In cases where DCU management access is lost due to a faulty SPP or SPM, you can use Oracle ILOM to change the roles of the controlling SPM.

Note - SPPs are hot-serviceable components that can be replaced at any time. SPMs are not serviceable components. To facilitate DCU-SPP failover on servers with SPM redundancy, two SPMs (SPM0 and SPM1) are provided for each DCU-SPP configuration.

For further about viewing DCU assignments or managing failover for DCU-SPP, see the following sections:

- [“View DCU Assignments and Manage Failover for DCU-SPP” on page 252.](#)
- [“Set DCU Failover Control for System ” on page 253](#)

▼ View DCU Assignments and Manage Failover for DCU-SPP

Before You Begin

- The Admin (a) role is required to change the roles of the active and standby DCU-SPM assignment.
- For a description of DCU health states, see [“DCU Status States” on page 254.](#)
- Changing the controlling SPM configuration might cause an interruption in communication between the DCU assigned Host and Oracle ILOM. If this occurs, any active KVMS sessions on the DCU-host will automatically be disconnected.

Note - Not all SPARC M series servers support SPM redundancy for DCU-SPP configurations.

1. To view the general health of all DCU assignments or to view the controlling SPM on a DCU, perform one of the following.

- **Web: From the active SP web interface, click System Information > DCUs.**

In the DCU table, view DCU location, Host-DCU assignment, and health details. For servers that support SPM redundancy, view the SPM that is actively assigned to manage the DCU system activity.

- OR -

- **CLI: From the active SP CLI, type:** `show /System/DCUs/DCU_n`

View these DCU properties: `health = location = host_assigned =`

If supported, view the controlling SPM property for the assigned DCU: `sp_name = /SYS/SPPn/SPMn`

For further details about the properties shown for the DCU target, type: **help /System/DCUs/DCU_n**

2. **To initiate failover of the controlling SPM for the DCU, perform one of the following:**
 - **Web: In the System Information > DCUs page, do the following:**
 1. In the DCU table select a DCU assignment then from the Actions list, select either Graceful Failover (negotiates the DCU-SPM assignment) or Forceful Failover (forcibly changes the DCU-SPM assignment).
 2. Click Apply.
If a prompt appears to confirm that you want to continue the failover operation. Click Yes to continue, otherwise click No.

- OR -
 - **CLI: Type: `set /Systems/DCUs/DCU_n initiate_sp_failover = true|force`**
Where *true* gracefully negotiates the DCU SPM assignment, where *force* forcibly changes the DCU-SPM assignment.
If a prompt appears to confirm that you want to continue the failover operation. Type **y** to continue, otherwise type **n**.

▼ Set DCU Failover Control for System

On SPARC servers, such as M8 series servers, you can set system-wide DCU failover control as of Oracle ILOM firmware version 4.0.1.x and later. By default, the system DCU failover control is automated by Oracle ILOM. However, during service operations such as hot-plug insertion or removal it might be helpful to suspend the automated failover control by Oracle ILOM. For these instances, the DCUs Failover control can be set to Manual. For further details, follow these instructions:

- **To set DCU system failover control, perform one of the following:**
 - **Web: From the active SP web interface, click ILOM Administration > Configuration Management > DCUs.**
In the Failover box, select Auto or Manual.
For a description of each option, see [“DCU System Failover Properties” on page 254](#).
- OR -
 - **CLI: From the active SP CLI, type:**

```
set /System/DCUs failover= Auto|Manual
```

For a description of each option, see [“DCU System Failover Properties” on page 254](#).

DCU Status States

For a list of possible health status states for logical DCU-host configurations, see the following table.

TABLE 81 DCU Health Status Definitions

Health Status	Definition
OK	The DCU assignment is in good working order.
Unknown	Oracle ILOM is unable to show the DCU health status, assignments, or sub-component details.
Service Required	Oracle ILOM has detected a problem on a chassis component, and a service action is required to resolve the issue. See the Open Problems page and view the knowledge base URL for resolution.
Warning	Oracle ILOM has detected a minor problem with the DCU assignment. Despite the warning message, the DCU assignment is functioning properly. The informational message can safely be ignored.

DCU System Failover Properties

TABLE 82 DCU Auto and Manual Failover Properties

System Failover Property	Definition
Auto	Automated failover by Oracle ILOM for DCUs is enabled.
Manual	Automated failover by Oracle ILOM for DCUs is disabled. Note: When the Failover property is set to Manual, Oracle ILOM is prevented from performing system initiated DCUs failover. Automated failover of the Active-SP is always enabled. For M7-4 and M8-4 systems, the Active-SP is also the controlling SP for DCU0, therefore, DCU0 failover might still occur in the context of an Active-SP failover (typically initiated by component health). When Failover is set to Manual, Oracle ILOM will automatically log the following event in cases when a DCU failover attempt would have been made if the Failover property was set to Auto:

System Failover Property	Definition
	Failover on /System/DCUs/DCU_x was not initiated by system due to auto-failover disabled by user.

PDomain and DCU Assignments

For SPARC servers, like the M series servers, you can use Oracle ILOM to view and manage logical Domain Configurable Unit (DCU) assignments for hosts. In addition, for SPARC servers, like the M7-16 servers, which support PDomain redundant service processor proxies (SPPs), you can use Oracle ILOM to change the controlling PDomain-SPP for a host. For further details about managing PDomain-DCU assignments, see the following information:

- [“Make DCUs Available For Assignment” on page 255](#)
- [“Assign Or Unassign DCUs To a PDomain Host” on page 256](#)
- [“Change Controlling PDomain-SPP for Host \(Failover\)” on page 258](#)

▼ Make DCUs Available For Assignment

Before You Begin

- The Admin (a) role is required to modify Host DCU assignments.
- You can make DCUs "available for assignment" to a host at any time, regardless of the Host and DCU state.
- To make DCUs "unavailable for assignment" to a host, the DCUs must not be assigned (in use) by the host.

To make DCUs available for assignment, follow these steps:

1. **Determine the DCU availability for each PDomain host by performing one of the following:**
 - **Web: Click the System Management > Domains.**
In the Host Configuration table of the Domains page, view the Assignable DCU column for each host.
 - **CLI: Type the following command string:**

```
show /Servers/PDomains/PDomain_n/host
```

View the `dcus_available` = property under the host target.
For further details about the CLI properties shown for a host target, type:

```
help /Servers/PDomains/PDomain_n/host
```

2. **To control which DCUs can be assigned to a PDomain host, perform one of the following:**

- **Web:** In the Host Configuration table, select a host and then click **Configure**.
For further instructions, click the *More details ...* link on the System Management > Domains page.

- **CLI:** Type the following command string:

```
set /Servers/PDomains/PDomain_n/host dcus_assignable= [/SYS/DCUn]
```

▼ Assign Or Unassign DCUs To a PDomain Host

Before You Begin

- The Admin (a) role is required to configure Host DCU assignments.
- Prior to assigning and unassigning DCUs to a Host, you must ensure that the Host on the assigned DCU is powered-off.

Note - Some servers support the configuration of non-Bounded PDomain (Expandable is set to *True*) and Bounded PDomain (Expandable is set to *False*). For further details about non-Bounded or Bounded PDomains, see the information in the administration guide provided with your server.

- The Reset and Host Control (r) role is required to modify the host power state.

To assign or unassign DCUs, follow these steps:

1. **Determine the current DCU assignments for hosts by performing one of the following:**

- **Web:** Click **System Management > Domains**.
In the Host Configuration table, view the Assigned DCU column and, if supported, the Expandable column.
For further details, click the *More details ...* link on the Domains page.

- **CLI:** Type the following command string:

```
show Servers/PDomains/PDomain_n/host
```

View the `dcus_assigned` = property under the host target.

2. **Power-down the PDomain host on the assigned DCU by performing one of the following:**

- **Web:** Click **System Management > Power Control** page, then click the *More details...* link on the **Power Control** page for further instructions.

- **CLI:** Type the following command string:

```
stop /Servers/PDomains/PDomain_n/host
```

3. **To assign or unassign DCU assignments to the powered-off host, perform one of the following:**

- **Web:** In the **System Management > Domains** page, click the *More details...* link for instructions.

- **CLI:** Perform one of the following

- **To assign a DCU, type the following command string:**

```
set /Servers/PDomains/PDomain_n/host dcus_assigned= [/SYS/DCUn]
```

To verify the status of the DCU assignment, type: `show /Servers/PDomains/PDomain_n/host`

View the `operation_in_progress` = property.

- **To unassign a DCU, type the following command string:**

```
set /Servers/PDomains/PDomain_n/host dcus_assigned= [/SYS/DCUn]
```

To verify that the specified DCU is unassigned, type: `show /Servers/PDomains/PDomain_n/host`

View the `dcus_available` = property under the host target.

4. **Start the PDomain host that was stopped in Step 2, for instance:**

- **Web:** Click the *More Details ...* link for instructions.

- **CLI:** Type the following command string:

```
start /Servers/PDomains/PDomain_n/host
```

▼ Change Controlling PDomain-SPP for Host (Failover)

Before You Begin

- Not all SPARC M series servers support PDomain-SPP failover. Therefore, if the Oracle ILOM properties described in this procedure do not appear in the CLI and web interface, the PDomain-SPP host failover feature is not supported. For further details about failover operations supported on a server, refer to the administration guide provided for the server.
- The Admin (a) role is required to change the controlling PDomain-SPP for host.
- Changing the controlling PDomain-SPP might cause an interruption in communication between the Host PDomain-SPP and Oracle ILOM. If this occurs, any active Oracle ILOM Remote System Console Plus sessions on the PDomain-SPP will automatically be disconnected.

To change the controlling PDomain-SPP that is currently responsible for managing Host system activity, follow these steps

1. Identify the active SPP for the PDomain by performing one of the following:

- **Web:** Click System Management > Domains page and view the SP Name column in the Host Configuration table.

- or -

- **CLI: Type:** `show /Servers/PDomains/PDomain_n/host`

View the `sp_name` = property to identify the active PDomain-SPP.

2. To change the controlling PDomain SPP for host, perform one of the following:

- **Web:** Click System Management > Domains page, then click the *More details...* link for instructions.

- or -

- **CLI: Type:** `set /Servers/PDomains/PDomain_n/host initiate_sp_failover=<true|force>`

Where *true* gracefully negotiates the PDomain-SPP assignment, where *force* forcibly changes the PDomain-SPP assignment. If a prompt appears to confirm that you want to continue the failover operation. Type *y* to continue, otherwise type *n*.

Redirecting Host Output to Rear VGA Port

Note - The policy for redirecting host output to a rear VGA port is not available on all Oracle servers. Also, the front and rear VGA ports on an Oracle server cannot be utilized simultaneously.

On some Oracle servers, Oracle ILOM provides a policy that enables you to redirect the host output to a VGA port on the rear panel of the server. By default, this policy is disabled and is only configurable from the Oracle ILOM CLI. For further details about setting this policy in Oracle ILOM CLI, see the following table.

TABLE 83 VGA Rear Port Property for Redirecting Host Output

User Interface Configurable Target and User Role:		
■ SP CLI: SP/policy		
■ User Role: Admin (a) role (required to modify the VGA rear port policy property).		
Note:		
■ The VGA rear port policy is not available on all Oracle servers.		
Property	Default	Description
VGA_REAR_PORT=	disabled	<i>disabled enabled</i>
■ disabled – When disabled, host output is prevented from being redirected to the VGA port on the rear panel of the server.		
■ enabled – When enabled, host output is redirected to the VGA port on the rear panel of the server.		
CLI Syntax for VGA Rear Port:		
set /SP/policy VGA_REAR_PORT=disabled enabled		

Related Information

- [“Navigating the Web Interface” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Navigating the Command-Line Interface \(CLI\) Namespace Targets” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Configuring Alert Notifications, Service Requests, or Remote Logging

Description	Links
Refer to this section for information about configuring, testing, and disabling alert notifications.	■ “Configuring Alert Notifications” on page 261
Refer to this section for configuration information for enabling Automatic Service Requests.	■ “Managing Automatic Service Requests” on page 267
Refer to this section for information about configuring a Syslog server to log Oracle ILOM events to a remote host.	■ “Configuring Syslog for Event Logging” on page 272

Related Information

- [“Managing Oracle ILOM Log Entries” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Managing SNMP Trap Alerts Using the Oracle ILOM” in Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x](#)
- [Table 40, “SNMP Configuration Properties,” on page 107](#)

Configuring Alert Notifications

System administrators can configure alert notifications in Oracle ILOM to provide advance warnings of possible system failures. Oracle ILOM supports the configuration of IPMI PET alerts, SNMP Trap alerts, and Email alert notifications.

Up to 15 alert notifications are configurable in Oracle ILOM using the Oracle ILOM CLI, Oracle ILOM web interface, or an SNMP client. For each configured alert notification, system administrators can optionally generate a test message to ensure that the destination recipient successfully receives the test message.

For further information about configuring alert notifications in Oracle ILOM, see the following topics:

- [“Alert Notification Configuration Properties” on page 262](#)
- [“Configure and Test Alert Notification \(IPMI PET, SNMP, or Email\)” on page 264](#)
- [“Disable Alert Notification \(IPMI PET, SNMP, or Email\)” on page 265](#)
- [“Configure SMTP Client for Email Alerts” on page 266](#)

Alert Notification Configuration Properties

For each alert notification, Oracle ILOM requires these three properties to be set: alert type, alert destination, and alert level. Depending on which alert type is configured, other properties are optionally configurable.

For further details about the configuration properties for alert notifications, see the following table.

TABLE 84 Alert Notification Configuration Properties

Property	Requirement	Description
Alert Type	Mandatory	The alert type property specifies the message format and the delivery method that Oracle ILOM will use when creating and sending the alert message. Alert type choices include: ■ IPMI PET Alerts – Required properties include: alert destination IP address and an alert level. Each specified alert destination must support the receipt of IPMI PET messages. ■ SNMP Trap Alerts – View alert management rules or change the alert management rule properties. Related Information: ■ “Managing SNMP User Accounts and SNMP Trap Alerts (CLI)” in <i>Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x</i> ■ “IPMI Alerts” in <i>Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x</i>
Alert Destination	Mandatory	The Alert Destination property specifies where to send the alert message. IP address destinations must be configured for IPMI PET and SNMP alerts. Email address destinations must be configured for Email alerts.
Alert Destination Port	Optional	The TCP/UDP destination port only applies to SNMP alert configurations. Oracle ILOM automatically selects a standard TCP/UDP destination port number. System administrators can optionally choose to accept the standard (162) port number or manually specify a TCP/UDP port number.
Alert Level	Mandatory	All alert notification configurations require setting an alert level. Alert levels enable the sending of the alert notification. In addition, for IPMI PET alerts and Email alerts, alert levels act as a filter mechanism to ensure alert recipients only receive the alert messages that they are most interested in receiving.

Property	Requirement	Description
		Oracle ILOM offers the following alert levels with Minor being the lowest alert offered: ■ Minor – Generates alerts for informational events, as well as major and critical events. ■ Major – Generates alerts for all non-critical, non-recoverable, and critical events. ■ Critical – Generates alerts for all critical and non-recoverable events. ■ Down – This level generates alerts for only upper and lower non-recoverable events. ■ Disable – Disables the alert configuration. Oracle ILOM will not generate an alert message. Important: Oracle ILOM supports alert level filtering for all IPMI PET alert configurations and Email alert configurations. Oracle ILOM does not support alert level filtering for SNMP alert configurations. However, to enable Oracle ILOM to generate an SNMP alert, one of the following alert levels must be specified: <i>Minor</i>, <i>Major</i>, <i>Critical</i>, or <i>Down</i>.
Email Custom Sender	Optional for Email Alerts	System administrators can optionally configure this property for Email alert configurations only. The email_custom_sender property enables Oracle ILOM to override the SMTP customer sender address by using one of the following strings: <IPADDRESS> or <HOSTNAME>. Example: alert@<IPADDRESS>.
Email Message Prefix	Optional for Email Alerts	System administrators can optionally configure this property for Email alert configurations only. The Email Message Prefix property enables Oracle ILOM to prepend user-specified information to the message body.
Event Class Filter	Optional for Email Alerts	System administrators can optionally configure this property for Email alert configurations only. The Event Class Filter property enables Oracle ILOM to filter out all information except the selected event class. To clear the filter and send information about all classes, enter empty double quotes ("").
Event Type Filter	Optional for Email Alerts	System administrators can optionally configure this property for Email alert configurations only. The Event Type Filter property enables Oracle ILOM to filter out all information except the selected event type. To clear the filter and send information about all event types, enter empty double quotes ("").
SNMP Version	Optional for SNMP Alerts	The SNMP Version property enables system administrators to specify the SNMP trap version being sent. Supported SNMP versions include: 1, 2c, or 3.
SNMP Community Name	Optional for SNMP Alerts	System administrators can optionally specify an SNMPv1 or 2c community string or an SNMPv3 user name.

Property	Requirement	Description
or		Note - If an SNMPv3 user name is configured, the SNMPv3 user name must be configured in Oracle ILOM. If the SNMP user name is not configured, the alert will not be authenticated for delivery.
User Name		

▼ Configure and Test Alert Notification (IPMI PET, SNMP, or Email)

The following procedure provides instructions for configuring and testing alert notifications using the Oracle ILOM CLI and web interface.

Before You Begin

- For Email alert configurations, the SMTP server must be configured. If the SMTP server is not configured, Oracle ILOM will not be able to generate Email alerts. For configuration details, see [“Configure SMTP Client for Email Alerts” on page 266](#).
- For SNMP alert configurations, the property for SNMP sets must be enabled and at least one user account must be configured for SNMP. For configuration details, see [Table 40, “SNMP Configuration Properties,” on page 107](#).
- Admin (a) role is required in Oracle ILOM to configure alert notification properties.

1. To populate the properties for one of the 15 alert configuration IDs, do the following:

■ Web:

Click ILOM Administration > Notifications > Alerts, click an Alert ID, and then click Edit. Define the required properties (level, type, and destination) and then click Save.

For required and optional property details, see [Table 84, “Alert Notification Configuration Properties,” on page 262](#).

■ CLI:

Type the following to set the required alert properties:

```
set /SP|CMM/alertmgmt/rules/n type=email|snmptrap|ipmipet destination=ip_address
port=required_for_snmptrap level=minor|major|critical|disable
```

For required and optional property details, see [Table 84, “Alert Notification Configuration Properties,” on page 262](#).

2. To test the configuration of an alert notification, do the following:

- **Web:**

Click ILOM Administration > Notifications > Alerts, click a configured Alert ID, and then click Test Rule.

A successful or failed status message appears.

- **CLI:**

Type the following to test a configured alert notification:

```
set /SP/CMM/alertmgmt/rules/n testalert=true
```

Note - When you test an alert notification rule, Oracle ILOM will send a test from all configured SNMP traps. Oracle ILOM does not have the ability to filter SNMP traps by destination.

A successful or failed status message appears.

Related Information:

- [Table 84, “Alert Notification Configuration Properties ,” on page 262](#)
- [“Configure SMTP Client for Email Alerts” on page 266](#)
- [Table 40, “SNMP Configuration Properties,” on page 107](#)
- [“Managing Oracle ILOM Log Entries” in *Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*](#)
- [“Managing SNMP Trap Alerts Using the Oracle ILOM” in *Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x*](#)

▼ Disable Alert Notification (IPMI PET, SNMP, or Email)

The following procedure provides instructions for disabling a configured alert notification using the Oracle ILOM CLI and web interface. For instructions for configuring and testing alert notifications from an SNMP application client, see [“View Component Information and the Oracle ILOM Event Log \(SNMP\)” in *Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x*](#).

Before You Begin

- Admin (a) role is required in Oracle ILOM to modify alert notification properties.

- **To disable the configuration of an alert notification, do the following:**

- **Web:**

Click ILOM Administration > Notifications > Alerts, click a configured Alert ID, and then click Edit. In the Level list box, click Disable, and then click Save.

A successful or failed status message appears.

- **CLI:**

Type the following to disable a configured alert notification:

```
set /SP|CMM/alertmgmt/rules/n level=disable
```

A successful or failed status message appears.

▼ **Configure SMTP Client for Email Alerts**

The following procedure describes how to configure Oracle ILOM as an SMTP client using the Oracle ILOM CLI and web interface. Oracle ILOM must act as an SMTP client to successfully send email alert notifications.

Before You Begin

- Prior to configuring Oracle ILOM as an SMTP client, determine the IP address and port number for the outgoing SMTP email server that will process the email notifications.
- The SMTP Client property for Custom Sender is optional. This property enables Oracle ILOM to override the SMTP sender address by using one of the following strings: `<IPADDRESS>` or `<HOSTNAME>`. For example: `alert@[IPADDRESS]`
- Admin (a) role is required in Oracle ILOM to configure SMTP Client properties.

- **To configure Oracle ILOM as an SMTP client, do the following:**

- **Web:**

Click ILOM Administration > Notifications > SMTP Client.

Enable the SMTP state, populate the required properties for the SMTP server IP address and port number, populate the optional property for Custom Sender if required, and then click Save.

- **CLI:**

Type:

```
set /SP|CMM/clients/smtp state=enable address=smtp_server_ip port=smtp_server_port  
custom_send=optional_string
```

Related Information:

- [“Configure and Test Alert Notification \(IPMI PET, SNMP, or Email\)” on page 264](#)

Managing Automatic Service Requests

Note - The Automatic Service Request properties in Oracle ILOM are *not* supported on all Oracle servers.

Oracle ILOM, as of firmware release 3.2.5, provides Automatic Service Request (ASR) configuration properties that enable Administrators to configure Oracle ILOM as an ASR Client. Upon configuring these properties, Oracle ILOM will automatically detect and forward fault event telemetry messages in real-time to Oracle Services. In addition, Oracle ILOM will forward a heartbeat message to Oracle Services every 24 hours to confirm that the managed server is powered-on and operational.

Administrators can choose to either: 1) connect the ASR Client in Oracle ILOM directly to Oracle Services by using the default ASR Manager Endpoint URL address provided; or 2) indirectly connect the ASR Client in Oracle ILOM to Oracle Services by setting the Endpoint URL address to an ASR Manager Relay.

For more information about configuring Oracle ILOM as an ASR Client, see the following sections:

- [“Configure Oracle ILOM as an ASR Client” on page 267](#)
- [“Manage Endpoint SSL Certificate Information” on page 268](#)
- [“Send an ASR Test or Heartbeat Message” on page 269](#)
- [“ASR Configuration Properties” on page 270](#)

▼ Configure Oracle ILOM as an ASR Client

Before You Begin

- The Admin (a) role is required to configure the ASR Client properties in Oracle ILOM.
- The ASR Client Endpoint URL property must be set to a registered ASR Manager or ASR Manager Relay.

Note - For further details about how to set up and register a system with Oracle ASR Manager, refer to the ASR product documentation at: https://docs.oracle.com/cd/E37710_01/install.41/e18475/ch2_asr_manager.htm#ASRUD128

- ASR is configurable from Oracle ILOM as either an ASR Client (as described in this topic) or as an SNMP management station (via ASR trap alert notifications). For more information about alternative methods for configuring ASR in Oracle ILOM, see the references listed in the Related Information section of this topic.
1. **Access the ASR configuration properties in Oracle ILOM:**
 - **Web:** Click ILOM Administration > Notification > ASR.
 - **CLI:** Type: `/SP/clients/asr`
 2. **Configure the ASR properties as described in Table 85, “ASR Client Properties,” on page 270.**
 3. **(Web interface only) Click Save.**

Related Information

- For information about configuring alert notifications as an alternative method to setting up Oracle ILOM as an ASR Client, see “Configuring Alert Notifications” on page 261.
- Use My Oracle Support to assign a contact and approve the ASR activation (<http://support.oracle.com>). For more information, refer to "How To Manage and Approve Pending ASR Assets" (Doc ID 1329200.1) at My Oracle Support (<http://support.oracle.com/rs?type=doc&id=1329200.1>).

▼ Manage Endpoint SSL Certificate Information

To verify the authenticity of the configured Endpoint URL, Oracle ILOM requires a local copy of a valid SSL Certificate.

- **For direct ASR Service Endpoint connections** (<https://transport.oracle.com>), Oracle ILOM provides (pre-installed) an SSL Certificate. If necessary, the Oracle-provided SSL Certificate can be replaced with a user-provided SSL Certificate.
- **For indirect ASR Service Endpoint connections**, a user-provided SSL Certificate must be uploaded to Oracle ILOM.

For details on how to load or remove an SSL Certificate, see the following instructions.

1. **Perform one of the following to enable the Strict Certificate Mode property.**
 - **Web:** Select the Strict Certificate Mode checkbox in the General Settings section of the ASR Client page.
 - **CLI:** Type the following command string:
`set /SP/clients/asr/ strictcertmode=disabled|enabled`
2. **Perform any of the following to locally manage the Endpoint SSL Certificate in Oracle ILOM:**
 - **To view the SSL Certificate:**
 - **Web:** In the Certificate Information section, view the Certificate File Status. If the status shows the certificate is *present*, click the *(details)* link for further certificate details.
 - **CLI:** Type:
`show /SP/clients/asr/cert cert_status`
 If status shows the certificate is present, type the following to view the certificate details:
`show /SP/clients/asr/cert`
 - **To load the SSL Certificate:**
 - **Web:** In the Certificate Information section, select a Transfer Method, provide the required information, and then click Load Certificate.
 For more details, see [“Supported File Transfer Methods” on page 50](#).
 - **CLI:** Under the /SP/clients/asr/cert target, type:
`load_uri=file_transfer_method://password@host/file_path/filename`
Where: The supported *file_transfer_method* can be one of the following: *ftp, tftp, ftp, sftp, scp, http, https*
 - **To remove the SSL Certificate:**
 - **Web:** In the Certificate Information section, click Remove Certificate.
 A message appears indicating that the certificate was removed.
 - **CLI:** Under the /SP/Clients/asr/cert target, type:
`set /SP/clients/asr/cert clear_action=true`
 When prompted, type *y* to continue the action or *n* to cancel the action.

▼ Send an ASR Test or Heartbeat Message

To manually send an ASR event message, the Status property must show "Registered."

1. Perform any of the following ASR event type actions:

- Send an ASR Test:
 - **Web:** Click Send Test.
The Oracle ILOM ASR client configuration transmits a test message to Oracle Services (Endpoint URL).
 - **CLI:** Type the following command string:

```
set /SP/clients/asr send-event=test
```
- Send an ASR Heartbeat:
 - **Web:** Click Send Heartbeat
The Oracle ILOM ASR client configuration transmits a heartbeat message to Oracle Services (Endpoint URL).
 - **CLI:** Type the following command string:

```
set /SP/clients/asr send-event=heartbeat
```

2. To verify that a test or heartbeat message was successfully sent, perform any of the following:

- Check for the ASR notification email.
- Check the entries in Oracle ILOM System Log for the applicable ASR Test event or ASR Heartbeat event.

ASR Configuration Properties

The following table describes the ASR CLI and Web interface properties in Oracle ILOM.

TABLE 85 ASR Client Properties

Property	Default	Description
Status (status=)	Not applicable, read-only property.	The Status identifies the operational state of the ASR Client in Oracle ILOM. Possible status values are: ■ Registered – The ASR Client in Oracle ILOM is properly configured and is enabled to communicate with Oracle Services (Endpoint URL). ■ Registration In Progress – The ASR Client in Oracle ILOM is in the process of registering with the specified Oracle Services ASR Manager (Endpoint URL). ■ Internal File Error – An internal file error occurred when Oracle ILOM attempted to transmit the telemetry messages to Oracle Services (Endpoint URL). For more details about this error, view the Oracle ILOM log files. ■ Not Running – The ASR Client State property in Oracle ILOM is currently set to disabled. ■ URL For Endpoint Not Configured – The Endpoint property is not currently configured with a URL address.

Property	Default	Description
		■ Username Not Configured – The Password property for the Oracle support account contract is not currently configured. ■ Password Not Configured – The Password property for the Oracle support account contract is not currently configured. ■ Invalid Registration Username and Password – The Username and Password properties for the Oracle support account contract are incorrectly configured. ■ Error Resolving Host – An error occurred when Oracle ILOM tried to resolve the Endpoint URL for the specified Oracle Services ASR Manager. For more details about this error, view the Oracle ILOM System Log.
State (state=)	Disabled	Disabled Enabled The ASR Client state must be enabled to send hardware telemetry messages to the specified Oracle Service (Endpoint URL). Disabling the ASR Client state prevents Oracle ILOM from sending hardware telemetry messages to Oracle Services. To enable the ASR Client State, select the State check box. CLI Syntax to Set ASR State set /SP/clients/asr state=enabled disabled
Endpoint (endpoint=)	https://transport.oracle.com	https://transport.oracle.com (default) user-specified Use the Endpoint property to directly or indirectly connect the ASR Client to Oracle Services. By default, the Endpoint property URL directly connects to the remote ASR Service at Oracle, which requires a username and password. Optionally, you can configure the Endpoint property to indirectly connect to the ASR Services by specifying the address of a local ASR Manager Relay. Note - Indirect endpoint configurations aggregate the telemetry data from many host instances. Endpoint URL Syntax Examples ■ <code>https http://asr_manager_host</code> ■ <code>https http://asr_manager_host:port_number/asr</code> CLI Syntax to Set Endpoint set /SP/clients/asr endpoint=https://transport.oracle.com ASR Manager Relay URL address Security Notes: ■ Direct Endpoint Connection (default) – Oracle ILOM uses a pre-installed SSL certificate to verify the authenticity of the direct Endpoint connection (https://transport.oracle.com). Users can choose to use the direct Endpoint pre-installed SSL Certificate provided by Oracle or replace it with a user-specified SSL Certificate. ■ Indirect Endpoint Connection – To verify the authenticity of an indirect Endpoint connection to the ASR Service at Oracle, a user-provided SSL Certificate must be uploaded to Oracle ILOM. For further details on how to upload or remove an SSL Certificate, see “Manage Endpoint SSL Certificate Information” on page 268.
Strict Certificate Mode	Enabled	Enabled (default) Disabled

Property	Default	Description
		The Strict Certificate Mode controls the validation of the Endpoint URL. When the Strict Certificate Mode is enabled, it requires a local copy of the Endpoint SSL Certificate. ■ Enable Strict Certificate Mode (default) — Select the Strict Certificate Mode check box to fully verify the digital signatures of the configured Endpoint SSL Certificate. ■ Disable Strict Certificate Mode — Clear the Strict Certificate Mode check box to provide limited validation of the ASR endpoint at the time of authentication over a secure channel.
Username & Password	Not applicable, user-defined.	Enter a valid My Oracle Support username (email address) and password. If you don't have a username, you can create a user account and register it with My Oracle Support at http://support.oracle.com. Note - If an invalid My Oracle Support account is specified, Oracle ILOM will not be able to successfully forward hardware telemetry messages detected from the managed server to Oracle Services. CLI Syntax to Set Username and Password set /SP/clients/asr username=user_defined password=user_defined
Proxy	Not applicable, user defined.	If you are using an HTTPS/HTTP proxy server to access the Internet, configure the following proxy server properties: Note - If you are <i>not</i> using a proxy server to access the Internet, you can leave the following proxy server properties blank. ■ Proxy Address — Specify an IP address or hostname and the port number of the proxy server. For example: (proxy_server_ip_address proxy_server_host_name):port_number ■ Proxy User Name — Specify the proxy server user name. ■ Proxy Password — Specify the password that is associated with the proxy server user name. Note - In cases where the following message appears, ASR Manager in relay mode is different from a proxy, ensure that the proxy server properties for the Oracle ILOM ASR Client are properly configured. CLI Syntax to Set Proxy set /SP/clients/asr proxy-host=user_defined proxy-user=user_defined proxy-password=user_defined

Configuring Syslog for Event Logging

Syslog is a protocol service used for logging events to a remote log host. System administrators can enable the Syslog service in Oracle ILOM by configuring a Syslog server IP address.

The events logged to a Syslog server provide all the same information that you would see in the local Oracle ILOM event log, including class, type, severity, and description. Oracle ILOM provides properties for configuring up to two Syslog servers.

▼ Configure Syslog IP Address for Event Logging

Before You Begin

- Admin (a) role is required in Oracle ILOM to modify syslog properties.
- To populate the IP address in one of the two Syslog properties, do the following:
 - **Web:**

Click ILOM Administration > Notifications > Syslog.

Type the IP address for the Syslog server in the Server 1 or Server 2 text box, and then click Save.
 - **CLI:**

Type:

```
set /SP | CMM/clients/syslog destination_ip=syslog_server_ip
```

Related Information:

- [“Managing Oracle ILOM Log Entries” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Setting System Management Power Source Policies and Device Monitoring

Description	Links
Refer to this section for descriptions of system management policies that are configurable from the server SP.	■ “Power-On and Cooling-Down Policies Configurable From the Server SP” on page 275
Refer to this section for descriptions of the system management policies that are configurable from the CMM.	■ “System Management Power Supply Policies Configurable From CMM” on page 278
Refer to this section to manage the Device Monitoring configuration.	■ “Setting Device Monitoring Configuration Properties” on page 280

Related Information

- [“Setting Power Alert Notifications and Managing System Power Usage” on page 283](#)

Power-On and Cooling-Down Policies Configurable From the Server SP

System administrators can optionally set system management policies from the server SP to control power-on and power-off policies on boot, as well as cooling policies for system components.

All system management policies are, by default, disabled from the Oracle ILOM SP. For property descriptions of the system management policies that are configurable from the server SP, see the following table.

Note - The policies described in this section are server-specific, therefore, they can vary from system to system. Consult the documentation provided with your server for additional policy details.

TABLE 86 Configurable Server SP Power-On and Cooling-Down Policies

User Interface Configurable Target and User Role:	
■ CLI: /SP/policy ■ Web: System Management > Policy > Policy Configuration ■ User Role: admin (a) (required for all property modifications)	
System Management Policy	Description
Auto-Power-On Host on Boot (HOST_AUTO_POWER_ON=)	<i>Disabled</i> (default) <i>Enabled</i> Enable this policy to automatically power on the host server operating system at boot. Note - Enabling this policy automatically disables the policy for “Set host power to last power state policy” if enabled. Note - The HOST_AUTO_POWER_ON property is <i>not</i> available for configuration on all x86 and SPARC servers. CLI Syntax for Auto-Power-On-Host on Boot: set /SP/policy HOST_AUTO_POWER_ON=enabled disabled
Set Host to Last Power State on Boot (HOST_LAST_POWER_STATE=)	<i>Disabled</i> (default) <i>Enabled</i> Enable this policy to set the host server power state to the last known state at boot. Note - Enabling this policy automatically disables the policy for “Auto power-on host policy” if enabled. Note - The HOST_LAST_POWER_STATE property is <i>not</i> available for configuration on all x86 and SPARC servers. CLI Syntax for Set Host to Last Power State on Boot: set /SP/policy HOST_LAST_POWER_STATE=enabled disabled
Set to Delay Host Power On (SPARC server only) (HOST_POWER_ON_DELAY=)	<i>Disabled</i> (default) <i>Enabled</i> Enable this policy on an Oracle SPARC server to delay the host operating system from powering on at boot. CLI Syntax for Set to Delay Power On: set /SP/policy HOST_POWER_ON_DELAY=enabled disabled
Set Low Line AC Override Mode Policy (x86 server only) (LOW_LINE_AC_OVERRIDE_MODE=)	<i>Disabled</i> (default) <i>Enabled</i> The Low Line AC Override policy determines whether a 4-CPU system can use low-line (110 volt) power for special testing scenarios. The power capacity for each power supply unit (PSU) is roughly 1000 watts at low line. Since the power of a 4-CPU system can exceed 1000 watts by a large amount, enabling this setting results in a loss of PSU redundancy. Note - The LOW_LINE_AC_OVERRIDE_MODE property is <i>not</i> configurable on all x86 servers. CLI Syntax for Set Low Line AC Override Mode Policy: set /SP/policy LOW_LINE_AC_OVERRIDE_MODE=enabled disabled

User Interface Configurable Target and User Role:

- CLI: */SP/policy*
- Web: **System Management > Policy > Policy Configuration**
- User Role: **admin (a)** (required for all property modifications)

System Management Policy	Description
Set Parallel Boot (Supported on most SPARC T series servers and SPARC 7-2 series servers) (PARALLEL_BOOT=)	<i>Enabled</i> (default) <i>Disabled</i> The PARALLEL_BOOT property enables the host to boot and power on in parallel with the SP. When enabled, parallel booting occurs if an auto-power policy (HOST_AUTO_POWER_ON or HOST_LAST_POWER_STATE) was on or if a user presses the power button while the SP is in the process of booting. Oracle ILOM must be running in order to enable the host to power on in these situations. When this property is set to disabled, the SP boots first, then the host boots. Note - The PARALLEL_BOOT property is <i>not</i> configurable on x86 servers or SPARC M series servers. It is configurable on most SPARC T series servers and the SPARC S7-2 series servers. CLI Syntax for Parallel Boot: set /SP/policy Parallel_Boot=enabled disabled
Redirect VGA Output (VGA_REAR_PORT=)	<i>Disabled</i> (default) <i>Enabled</i> Note - The VGA_REAR_PORT property is <i>not</i> configurable on x86 servers or SPARC M series servers. It is configurable on most SPARC T series servers and the SPARC S7-2 series server. Enable to redirect vga output to the rear port of the server. CLI Syntax for VGA OUTPUT: set /SP/policy VGA_REAR_PORT=enabled disabled
Set Enhanced PCIe Cooling Mode (x86 server only) (ENHANCED_PCIE_COOLING_MODE=)	<i>Disabled</i> (default) <i>Enabled</i> Set to allow the host to poweron independently of ILOM Enable this policy on an Oracle x86 server PCIe card systems to satisfy cooler operating temperature requirements. The PCIe cool-down policy mode, when enabled, directs Oracle ILOM to lower the chassis output temperature sensor thresholds to keep the PCIe cards operating within the required temperature range. Note - The ENHANCED_PCIE_COOLING_MODE property is <i>not</i> configurable on all x86 servers. CLI Syntax for Set Enhanced PCIe Cooling Mode: set /SP/policy ENHANCED_PCIE_COOLING_MODE=enabled disabled
Enable a Cooldown Period Before Host Shuts Down (SPARC server only) (HOST_COOLDOWN=)	<i>Disabled</i> (default) <i>Enabled</i> Enable this property on SPARC servers to enter a cool down mode upon powering off the host server. The cool down mode directs Oracle ILOM to monitor certain components to ensure that they are below a minimum

User Interface Configurable Target and User Role:

- CLI: `/SP/policy`
- Web: System Management > Policy > Policy Configuration
- User Role: admin (a) (required for all property modifications)

System Management Policy	Description
	temperature as to not cause harm to the user. Once the server sub-components are below the minimum temperature, the power is removed from the server, or the host will turn off if the process takes longer then 4 minutes to complete.
	CLI Syntax to Enable Cool Down Period Before Host Shuts Down:
	<code>set /SP/policy HOST_COOLDOWN=enabled disabled</code>

System Management Power Supply Policies Configurable From CMM

System administrators can optionally set system management policies from the CMM to manage chassis power supply demand, power supply fan speeds, storage blade SAS-2 capability, and chassis power management.

For property descriptions of the system management policies that are configurable from the CMM, see the following table:

TABLE 87 Configurable CMM Power Supply Policies

User Interface Configurable Target and User Role:		
■ CLI: <code>/CMM/policy - or - /CH/BLn/SP/policy</code> ■ Web: System Management > Policy > Policy Configuration ■ User Role: admin (a) (required for all property modifications)		
System Management Policy	Default	Description
Light Load Efficiency Mode (<code>LIGHT_LOAD_EFFICIENCY_MODE=</code>)	Disabled	<i>Disabled Enabled</i> Enable this policy to: 1) monitor the chassis system power usage; and 2) automatically shut down the power supply unit sides to achieve higher efficiency. CLI Syntax for Light Load Efficiency Mode: <code>set /CMM/policy LIGHT_LOAD_EFFICIENCY_MODE=enabled disabled</code>
Monitor Power Supply 0 Side 0 for power (<code>MONITOR_PS0_SIDE0=</code>)	Enabled	<i>Disabled Enabled</i> Enable this policy to enable monitoring of Power Supply 0 Side 0 under Light Load Efficiency Mode.

User Interface Configurable Target and User Role:

- CLI: /CMM/policy - or - /CH/BLn/SP/policy
- Web: System Management > Policy > Policy Configuration
- User Role: admin (a) (required for all property modifications)

System Management Policy	Default	Description
CLI Syntax for Monitor Power Supply 0 Side 0:		
set /CMM/policy MONITOR_PS0_SIDE0=enabled disabled		
Monitor Power Supply 0 Side 1 for power (MONITOR_PS0_SIDE1=)	Enabled	Disabled Enabled Enable this policy to enable monitoring of Power Supply 0 Side 1 under Light Load Efficiency Mode.
CLI Syntax for Monitor Power Supply 0 Side 1:		
set /CMM/policy MONITOR_PS0_SIDE1=enabled disabled		
Monitor Power Supply 1 Side 0 for power (MONITOR_PS1_SIDE0=)	Enabled	Disabled Enabled Enable this policy to enable monitoring of Power Supply 1 Side 0 under Light Load Efficiency Mode.
CLI Syntax for Monitor Power Supply 1 Side 0:		
set /CMM/policy MONITOR_PS1_SIDE0=enabled disabled		
Monitor Power Supply 1 Side 1 for power (MONITOR_PS1_SIDE1=)	Enabled	Disabled Enabled Enable this policy to enable monitoring of Power Supply 1 Side 1 under Light Load Efficiency Mode.
CLI Syntax for Monitor Power Supply 1 Side 1:		
set /CMM/policy MONITOR_PS1_SIDE1=enabled disabled		
Cooling Door Installed (COOLING_DOOR_INSTALLED=)	Disabled	Disabled Enabled Enable this policy to support a cooling door installed on a Sun Blade 6048 chassis.
CLI Syntax for Cooling Door Installed:		
set /CMM/policy COOLING_DOOR_INSTALLED=enabled disabled		
Force Power Supply Fans to High Speed (PS_FANS_HIGH=)	Disabled	Disabled Enabled Enable this policy to force the power supply fans to 100% capacity.
CLI Syntax for Force Power Supply Fans to High Speed:		
set /CMM/policy PS_FANS_HIGH=enabled disabled		
Force Power Supply Fans to Low Speed (PS_FANS_LOW=)	Disabled	Disabled Enabled Enable this policy to force the power supply fans to 80% capacity.

User Interface Configurable Target and User Role:

- CLI: /CMM/policy - or - /CH/BLn/SP/policy
- Web: System Management > Policy > Policy Configuration
- User Role: admin (a) (required for all property modifications)

System Management Policy	Default	Description
CLI Syntax for Force Power Supply Fans to Low Speed:		
set /CMM/policy PS_FANS_LOW=enabled disabled		
Force Server Blade to be SAS2 Capable at 3Gbps. (FORCE_SAS2_3GBPS=)	Disabled	<i>Disabled Enabled</i> Enable this policy to force the NEM(s) to run the SAS link at a slower rate, for those rare cases when this action is necessary. CLI Syntax for Force Server Blade to be SAS2 Capable at 3Gbps: set /CH/BLn/SP/policy FORCE_SAS2_3GBPS=enabled disabled
Manage chassis power. Caution - Disabling may lead to chassis shutdown. (POWER_MANAGEMENT=)	Enabled	<i>Disabled Enabled</i> Enable this policy to determine whether there is enough power in the chassis to power on a new server module installed in the chassis. CLI Syntax for Manage Chassis Power: Caution - Disabling may lead to chassis shutdown. set /CMM/policy POWER_MANAGEMENT=enabled disabled

Related Information

- [“CMM Web Interface: Blade Server Views” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Managing Blade Servers From the CMM CLI” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Setting Device Monitoring Configuration Properties

Note - The Device Monitor feature is not available for configuration on all Oracle Servers. This feature applies to supported Oracle storage controllers, such as the Oracle Flash Accelerator F640 PCIe Card and 6.4 TB NVMe SSD device.

As of Oracle ILOM firmware version 4.0.3, administrators can optionally choose to enable or disable device monitoring. Device monitoring is enabled by default. For a description of the device monitoring configuration properties, see the following table:

TABLE 88 Configurable Device Monitoring Properties

User Interface Configurable Target and User Role:	
■ CLI: /SP/services/device_monitor ■ Web: System Management > Device Monitor ■ User Role: admin (a) (required for all property modifications)	
System Management Policy	Description
Service State (servicestate=)	Note - The Device Monitor feature is <i>not</i> available for configuration on all Oracle Servers. Enabled (Default) Disabled Suspended ■ Enabled –Select Enabled to enable the device monitoring mode in Oracle ILOM. When enabled, Oracle ILOM will manage the supported device (s) at the set polling interval, as well as report errors and faults detected for these devices in the Open Problems web page and CLI target (show /System/Open_Problems). ■ Disabled –Select Disabled to disable the device monitoring mode in Oracle ILOM.. ■ Suspended –Select Suspended to temporarily suspend the device monitoring mode in Oracle ILOM. When this mode is suspended, device monitoring will remain in a suspended state until after the SP reboots or the Service State is set to Enabled. During this time period, all alert and error notifications generated by device monitoring are also suspended. CLI Syntax for Device Monitor Service State: set /SP/services/device_monitor servicestate=enabled disabled suspended
Polling Interval (polling_interval=)	60 seconds (Default) The Polling Interval property indicates how frequently Oracle ILOM will poll the supported device(s). This property is only in effect when the Service State property is enabled. Seconds (60 default) – Enter a value from 30 to 600 to specify the number of seconds Oracle ILOM will wait before repolling the supported device(s). CLI Syntax for Device Monitor Polling Interval: set /SP/services/device_monitor polling interval= [30 to 600]

Setting Power Alert Notifications and Managing System Power Usage

Description	Links
Refer to this section for descriptions of CMM and SP configurable properties for power consumption alert notifications.	■ “Setting Power Consumption Alert Notifications” on page 283
Refer to these sections for descriptions of CMM and SP configurable properties for managing system power usage.	■ “Setting CMM Power Grant and SP Power Limit Properties” on page 284 ■ “Setting SP Advanced Power Capping Policy to Enforce Power Limit” on page 287 ■ “Setting SP Power Management Settings for Power Policy (SPARC)” on page 289 ■ “Setting the CMM Power Supply Redundancy Policy” on page 291

Related Information

- [“Real-Time Power Monitoring Through Oracle ILOM Interfaces” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Configuring Alert Notifications, Service Requests, or Remote Logging” on page 261](#)

Setting Power Consumption Alert Notifications

Oracle ILOM provides configuration properties for power consumption alert notifications. When the configuration properties are enabled, configured email recipients receive alert notifications when the system power exceeds the set threshold(s).

Power consumption thresholds and Email alert notifications are configurable from the Oracle ILOM CLI or web interface.

For details about configuring an email alert notification, see [“Configuring Alert Notifications” on page 261](#).

For details about configuration properties for power notification thresholds, see the following table.

TABLE 89 Power Consumption Notification Threshold Configuration Properties

User Interface Configurable Target and User Role;		
■ SP CLI: /SP/CMM /powermgmt ■ Web: Power Management > Consumption > Notification Threshold 1 2 ■ Admin (a) role (required to modify threshold properties).		
Requirements:		
■ To apply threshold property modifications in the web interface, you must click Save. ■ Email alert notification properties must be configured in Oracle ILOM.		
Property	Default	Description
Notification Threshold 1 and 2 (threshold1= <i>n</i> threshold2= <i>n</i>)	Disabled	<i>Disabled</i> <i>Enabled</i> ■ Disabled – When disabled, the Notification Threshold property state and wattage property value (0) are disabled. ■ Enabled – When enabled, the Notification Threshold property state and the user-specified wattage property value are configurable. Specify a wattage threshold value between 1 and 65535. Oracle ILOM generates an alert event if the power on the system exceeds the set threshold. If an email alert recipient is configured, Oracle ILOM also generates a power consumption email alert to the configured recipient. CLI Syntax for Power Consumption Notification Threshold set /SP/CMM/powermgmt threshold1=<0 to 65535> threshold2=<0 to 65535> Related Information: ■ “Configuring Alert Notifications” on page 261 ■ “Power Consumption Terminology and Properties” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x

Setting CMM Power Grant and SP Power Limit Properties

Oracle ILOM provides SP and CMM configurable properties for limiting and granting power use on a managed system. These power limiting and power granting properties are configurable from the Oracle ILOM CLI and web interface as of firmware version 3.1.1 or later.

For further information about the configurable properties in Oracle ILOM for power limiting and power granting, see the following procedures.

- [“Set CMM Blade Slot Grant Limit Property” on page 285](#)

- [“Set SP Power Target Limit Properties” on page 286](#)

▼ Set CMM Blade Slot Grant Limit Property

Before You Begin

- Oracle ILOM CMM firmware version 3.1.1 or later is required.
- The Admin (a) role is required in Oracle ILOM to modify the Blade Slot Grant limit property.
- The Blade Slot Grant Limit property controls the amount of power the CMM will permit a CPU blade server to consume. By default, the Blade Slot Grant Limit is set to 1200 watts (maximum blade slot power limit).

System administrators can choose to accept the default blade slot grant limit (1200 watts) or modify it. However, the grant limit property must not be set less than the blade slot power wattage already granted by the CMM (granted power). Setting the Blade Slot Grant Limit to 0 prevents the installed CPU blade server from powering-on.

Note - The Blade Slot Grant Limit is ignored by installed storage blade servers. The storage blade servers are auto-powered.

This procedure provides both web and CLI CMM instructions.

- **To set the CMM blade slot grant limit property, perform one of the following Oracle ILOM interface procedures:**

Oracle ILOM Interface	Set CMM Blade Slot Grant Limit Procedure
Web	1. Click Power Management > Allocation. 2. In the Power Grants table, click the radio button adjacent to a CPU blade server, then click Edit. Note. Storage blade servers appear in the table as “Ignored Auto-Powered blade.” The Blade Slot Grant Limit property is ignored for storage blade servers. 3. In the Edit dialog, enable one of the following Blade Slot Grant Limit options: Slot Maximum (default,1200 watts) – When enabled, the CMM can grant up to 1200 watts of power to the requesting CPU blade server. - or - Custom - When enabled, type a number for the permitted power wattage that the CMM can grant to a requesting CPU blade server. The power wattage number must not be less than the power wattage number already granted to the blade slot by the CMM (granted power). Setting the power wattage to 0 will prevent the installed CPU blade server from powering-on.

Oracle ILOM Interface	Set CMM Blade Slot Grant Limit Procedure
	4. Click Save to apply the changes.
CLI	Type: <pre>set /CMM/powermgmt/powerconf/bladeslots/BLn grant_limit=watts</pre> Where: n – Type the blade slot number of an installed CPU blade server. watts – Type a number for the permitted power wattage that the CMM can grant to a requesting CPU blade server. The power wattage number must not be less than the power wattage number already granted to the blade slot by the CMM (granted power). Setting the power wattage to 0 will prevent the installed CPU blade server from powering-on.

Related Information

- [“Power Consumption Terminology and Properties” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Monitoring Power Allocations” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- CMM Policy for Managing Chassis Power, [“System Management Power Supply Policies Configurable From CMM” on page 278](#)
- [“Getting Started With Oracle ILOM” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

▼ Set SP Power Target Limit Properties

Before You Begin

- Oracle ILOM SP firmware version 3.1.2 or later must be installed on the managed server.
- The Admin (a) role is required in Oracle ILOM to modify the Power Limit properties.
- The Power Target Limit on the SP is disabled by default.

The Power Target Limit, when enabled, controls the amount of power the managed server is permitted to consume.

This procedure provides both web and CLI SP instructions.

- **To enable the SP Power Target Limit properties, perform one of the following Oracle ILOM interface procedures:**

Oracle ILOM Interface	Set Power Target Limit Procedure
Web	1. Click Power Management > Power Limit.

Oracle ILOM Interface	Set Power Target Limit Procedure
	- Enter a target limit value in watts or a percentage. The target limit should be set between the minimum power drawn by the installed hardware components and the maximum power the managed server is permitted to consume (peak permitted). - Enable the activation state for Power Limiting. The Power Limiting state must be enabled for Oracle ILOM to activate the target power limit configuration. - Click Save to apply the changes. - To enforce the set power limit property on the SP, see “Set Advanced Power Capping Policy” on page 288.
CLI	- Type: set /SP/powermgmt/budget pending_power_limit=value pendingactivation_state=enabled commit_pending=true Where <i>value</i> is either the wattage target limit value or percentage target limit value. The target limit should be set between the minimum power drawn by the installed hardware components and the maximum power the managed server is permitted to consume (peak permitted). - To enforce the set power limit property on the SP, see “Set Advanced Power Capping Policy” on page 288.

Related Information

- [“Monitoring Power Allocations” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Setting SP Advanced Power Capping Policy to Enforce Power Limit” on page 287](#)
- [“Getting Started With Oracle ILOM” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)

Setting SP Advanced Power Capping Policy to Enforce Power Limit

Oracle ILOM provides an Advanced Power Capping Policy on the SP that helps to enforce the system target power limit. System administrators can choose to set either a soft cap with a grace period or a hard cap to keep the peak permitted power consumption under the target power limit. In addition, system administrators can set violation actions for when the set Power Capping Policy is violated.

The Power Capping Policy properties are configurable from the Oracle ILOM CLI and Web interface as of firmware version 3.1.1 or later. For further information about how to configure the Power Capping Policy properties in Oracle ILOM, see the following procedure.

▼ Set Advanced Power Capping Policy

Before You Begin

- Oracle ILOM SP firmware version 3.1.1 or later is required.
- The Power Limit (power_limit) property must be set on the server prior to setting the Power Capping Policy. For details, see [“Set SP Power Target Limit Properties” on page 286](#).
- The Admin (a) role is required in Oracle ILOM to modify the Advanced Power Capping Policy properties.

Note - An overly aggressive Soft Power Capping Policy might produce an excessive amount of ILOM log entries that are related to assertion and deassertion of the power budget status (/SYS/PWRBS) sensor. To reduce these log entries shown in the ILOM log file, consider increasing the properties for either the Power Target Limit or Soft Cap Policy, or both.

This procedure provides both web and CLI SP instructions.

- **To set the SP Power Capping Policy, perform one of the following Oracle ILOM interface procedures:**

Oracle ILOM Interface	Set Power Capping Policy (Soft Cap, Hard Cap, and Violation Actions) Procedure
Web	- Click Power Management > Power Limit. - Enable one of the following Advanced Power Capping Policy options: Soft Cap (default) - When enabled, the system power is capped only if the system power consumption (Actual power) exceeds the target power limit and the user-configurable grace period (default, 10 seconds). System administrators can choose to accept the default grace period of 10 seconds or modify the default grace period by clicking Custom and entering the allowable grace period seconds (1 to 99999). - or - Hard Cap – When enabled, the system power consumption is capped to keep the Peak Permitted Power under the target power limit. - Enable one of the following Policy Violation Actions: None (default) – When enabled, no action is taken when the system power consumption violates the Power Policy. - or - Hard Power Off – When enabled, the system is immediately powered off when the system power consumption violates the Power Policy. - Click Save to apply the changes.
CLI	To set a Soft Cap or Hard Cap value for the Power Capping Policy type: <pre>set /SP/powermgmt/budget pendingtimelimit=default integer between 1 and 99999 0 commit_pending=true</pre>

Oracle ILOM Interface	Set Power Capping Policy (Soft Cap, Hard Cap, and Violation Actions) Procedure
	Where: <i>default</i> or <i>integer between 1 and 99999</i> is a Soft Cap value – The power capping policy is set to Soft Cap by default with a default time limit of 10 seconds. When a Soft Cap value is set (default or 1 to 99999), the system power is capped only if the system power consumption (Actual power) exceeds the target power limit and the user-configurable <i>timelimit</i> property (default, 10 seconds). - or - <i>0</i> is a Hard Cap value – When set to 0, the system power consumption is capped to keep the Peak Permitted Power under the target power limit. 2. To set a value for <i>violation_actions</i>, type: <pre>set /SP/powermgmt/budget pendingviolation_actions=<i>none hardpoweroff</i> commit_pending=true</pre> Where: <i>none hardpoweroff</i> – Type <i>none</i> for the system to take no action if the power policy is violated. Type <i>hardpoweroff</i> to immediately power off the system if the system power consumption violates the power policy.

Related Information

- “Power Consumption Terminology and Properties” in *Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*
- “Monitoring Power Allocations” in *Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*
- “System Management Power Supply Policies Configurable From CMM” on page 278
- “Getting Started With Oracle ILOM” in *Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*

Setting SP Power Management Settings for Power Policy (SPARC)

Oracle ILOM provides SP Power Management Settings to enable a system administrator to tune the power policy settings to match the system's performance requirements.

For further information about the configurable properties in Oracle ILOM for setting SP Power Management Settings, see the following procedure.

▼ Set Power Management Settings for Power Policy on SPARC Servers

Before You Begin

- The Admin (a) role is required in Oracle ILOM to modify the power management properties.
- The Power Management Settings for Power Policy is supported only on SPARC servers.
- As of Oracle ILOM 3.2.1, the Performance policy setting requires the Oracle VM Server for SPARC (Logical Domains Manager) 3.0 or later software to be installed on the primary domain. If an earlier version is installed, the Performance policy setting will behave as if the power management policy is set to Disabled.

This procedure provides both web and CLI SP instructions.

- To set the Power Management Settings, perform one of the following Oracle ILOM interface procedures:

Oracle ILOM Interface	Set Power Management Settings for Power Policy Procedure
Web	1. Click Power Management > Settings. 2. Enable one of the following Power Policy options: Disabled – When the policy setting is set to Disabled, all system components will run at full speed and power capacity. Performance – When the policy setting is set to Performance, unused and idle components in the system are placed into a slower speed or sleep state resulting in greater power savings with little impact on performance. Elastic – When the policy setting is set to Elastic, the system's power usage adapts to the current utilization level of the components. Components are brought into or out of a slower speed or a sleep state to match the system's utilization for those components. 3. Click Save to apply the changes.
CLI	1. Type the following to set the Power Management Policy: set /SP/powermgmt policy=disabled performance elastic When: policy=disabled is set, all components in the system will run at full speed and power capacity. policy=performance is set, unused and idle components in the system are placed into a slower speed or sleep state resulting in greater power savings with little impact to performance. policy=elastic is set, the system's power usage adapts to the current utilization level of the components. Components are brought in to or out of a slower speed or a sleep state to match the system's utilization for those components.

Related Information

- [“Power Consumption Terminology and Properties” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- [“Monitoring Power Allocations” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x](#)
- CMM Policy for Managing Chassis Power, [“System Management Power Supply Policies Configurable From CMM” on page 278](#)

Setting the CMM Power Supply Redundancy Policy

Oracle ILOM provides a CMM Power Supply Redundancy Policy to prevent the loss of power to blade system chassis components. The Power Supply Redundancy Policy is configurable from the Oracle ILOM CMM CLI and web interface.

For further information about configuring a Power Supply Redundancy Policy for a blade system chassis from the Oracle ILOM CMM, see the following procedure.

▼ Set CMM Power Supply Redundancy Policy

Before You Begin

- Oracle ILOM CMM firmware version 3.1.1 or later is required.
- A minimum of two power supply units (PSU) must be initially installed within the blade system chassis to support the Power Supply Redundancy Policy.

Note - The Sun Blade 6000 PSUs contain two power sides. The Sun Blade 6048 PSU contains three power sides. It is possible for system administrators to shut down one side of the PSU by enabling the system management policy for Light Load Efficiency Mode (LLEM). The LLEM supports both redundant and non-redundant PSUs.

- The Admin (a) role is required in Oracle ILOM to modify the CMM grant limit property.
- The Power Supply Redundancy Policy controls the amount of power the CMM reserves from each PSU in case of a PSU failure. The CMM Power Supply Policy is set, by default in Oracle ILOM, to reserve half the power (N+N) from each PSU. If a PSU fails within the blade chassis, the CMM allocates the reserved power from the remaining PSU to prevent a power loss to the chassis system components.

System administrators can choose to accept the default Power Supply Redundancy Policy (N+N) or disable it.

Note - When the PSU redundancy policy is modified, the modification will affect the power wattage the CMM is permitted to allocate to the CPU blade servers. For instance, when the redundancy policy is enabled (N+N), the CMM will re-adjust the Peak Permitted power to the wattage the PSU(s) can provide minus the wattage being reserved. If the redundancy policy is disabled and a PSU fails, the CMM will reduce the wattage for the Peak Permitted system power. If the Peak Permitted system wattage is reduced below the already Allocated Power wattage, the system administrator should take steps to power off the CPU blade servers to reduce the chassis power allocation.

This procedure provides both web and CLI CMM instructions.

- **To set the CMM Power Supply Redundancy Policy, perform one of the following Oracle ILOM interface procedures:**

Oracle ILOM Interface	Set CMM PSU Redundancy Policy Procedure
Web	1. Click Power Management > Redundancy. 2. Enable one of the following power redundancy policies: N+N (default) – When enabled, the CMM reserves half the power from each chassis PSU for power redundancy. - or - None – When enabled, the redundant PSU policy configuration is disabled. 3. Click Save to apply the changes.
CLI	■ Type: <code>set /CMM/powermgmt redundancy=redundancy none</code> Where: redundancy (default) – When set, the CMM reserves half the power from each chassis PSU for power redundancy. none – When set, the redundant PSU policy configuration is disabled.

Related Information

- Force CMM Power Supply Fan Speeds, [“System Management Power Supply Policies Configurable From CMM” on page 278](#)
- CMM Policy for Managing Chassis Power, [“System Management Power Supply Policies Configurable From CMM” on page 278](#)

Performing Oracle ILOM Maintenance and Configuration Management Tasks

Description	Links
Refer to this section for information about performing firmware updates for upgradable system devices.	■ “Updating Oracle ILOM Firmware” on page 293
Refer to this section for information about resetting the power on the SP, CMM, or blade chassis components.	■ “Reset Power to Service Processor or Chassis Monitoring Module ” on page 301
Refer to this section for enabling or disabling server properties for ASR qualified components, as well as redundancy roles for active and standby server SPs.	■ “Managing ASR Component States” on page 303 ■ “Managing Active and Standby SP Redundancy Roles (SPARC)” on page 304
Refer to this section for instruction for backing up, restoring or resetting an SP or CMM Oracle ILOM configuration.	■ “Backing Up, Restoring, or Resetting the Oracle ILOM Configuration” on page 306

Related Information

- [“Taking a Snapshot: Oracle ILOM SP State” in *Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*](#)

Updating Oracle ILOM Firmware

To ensure that users have access to the latest Oracle ILOM features and product enhancements, all upgradable system devices should be updated with the latest Oracle ILOM firmware release.

System administrators can update the firmware for any upgradable system device using the Oracle ILOM web interface or CLI.

For further details about Oracle ILOM firmware updates, see these topics:

- [“Firmware Upgradable Devices” on page 294](#)
- [“Preserve Oracle ILOM Configuration ” on page 294](#)

- [“Before You Begin the Firmware Update” on page 295](#)
- [“Update the Server SP or CMM Firmware Image” on page 296](#)
- [“Update Blade Chassis Component Firmware Images” on page 298](#)
- [“Recover From a Network Failure During Firmware Update” on page 301](#)

Firmware Upgradable Devices

Firmware images are available on the Oracle product download web site for the following Oracle ILOM managed devices:

- Rackmount or blade servers (x86 and SPARC) that contain a service processor (SP)
- Blade system chassis monitoring module (CMM)
- Blade system chassis network expansion modules (NEMs) that include a service processor
- Blade system chassis storage blade servers

For firmware download instructions, refer to [“Oracle ILOM Firmware Versions and Download Methods” in Oracle ILOM Feature Updates and Release Notes Firmware Release 4.0.x](#) [“Oracle ILOM Firmware Versions and Download Methods” in Oracle ILOM Feature Updates and Release Notes Firmware Release 4.0.x](#).

Preserve Oracle ILOM Configuration

When updating to a later firmware release, the Preserve Configuration option (when enabled) saves your existing Oracle ILOM configuration and restores the user-defined configuration settings after the firmware update completes. However, when the Preserve Configuration option is not enabled, the Oracle ILOM configuration settings (including network settings) are reset to their factory default values upon completing the firmware update process.

Note - The term *configuration* refers to the settings configured in Oracle ILOM by a user. These settings can include user account settings, SP network settings, management access settings, alert configuration settings, remote management configurations, and so on.

If you are updating to a prior firmware release and Oracle ILOM detects a preserved configuration for that release, the Preserve Configuration option (when enabled) reverts to the configuration for the prior release after the update process completes.

Generally, you should not update the firmware on your system to a prior release. However, if you determine that you need to run an earlier version of the firmware on your system, you can update the firmware to any prior firmware release that is available for download.

Before You Begin the Firmware Update

Prior to updating the Oracle ILOM firmware, you should:

1. Verify that the managed server SP or CMM has network connectivity to update the firmware image.

For example, to verify that the server SP or CMM is connected to the network, use a remote web browser client or a remote CLI ssh client to log in to the server SP or CMM. For instruction, see [“Log In to the Oracle ILOM SP or CMM” on page 36](#).

2. Identify the Oracle ILOM firmware version that is running on the managed device (server SP, storage server, NEM SP, or CMM).

The firmware version for all upgradable devices appears in the Firmware page in the web interface or in the `/System/Firmware` CLI target.

3. Download the firmware image for the upgradable device from the Oracle product download web site and then place the image on a local or network share or on a TFTP, FTP, HTTP or HTTPS server.

For firmware download instructions, refer to [“Oracle ILOM Firmware Versions and Download Methods” in Oracle ILOM Feature Updates and Release Notes Firmware Release 4.0.x](#).

4. Obtain an Oracle ILOM user name and password that has Admin (a) role account privileges. You must have Admin (a) privileges to update the firmware image.
5. Notify SP or CMM users of the scheduled firmware update and ask them to close all client sessions until after the firmware update is complete.

System administrators can use a banner message to communicate this message to users. For instructions for creating and enabling a banner message at login, see [“Management of Banner Messages at Log-In” on page 94](#).

6. If required by the host server platform, power off the host operating system before updating the SP firmware image.

To determine if the host needs to be powered off, refer to the firmware update section in the administration guide provided for the server.

Note that if the host server power is ON and the platform server requires the power to be OFF, click the button in the Actions panel on the Summary web page to gracefully power off the host operating system and server. Alternatively, you can gracefully power off the host operating system and server from the CLI by issuing the following command:

```
stop /System
```

▼ Update the Server SP or CMM Firmware Image

System administrators can choose to start the firmware update process for upgradable devices from the web interface Actions panel, the Maintenance Firmware Upgrade page, or a CLI target.

The following procedure explains the firmware update process using the CLI and the web interface Maintenance page.

Before You Begin

- Ensure that the initial requirements for updating the SP or CMM firmware image have been met. See [“Before You Begin the Firmware Update” on page 295](#).
- The firmware update process takes several minutes to complete. During this time, do not perform any other Oracle ILOM tasks. When the firmware update process complete, the system will either reboot or power-off.

To start the firmware update process and to verify that the update process has completed successfully, follow these steps:

1. **To start the firmware update process for a server SP or CMM image, perform the following steps using one of the Oracle ILOM interfaces:**

Oracle ILOM Interface	To Start and Run Firmware Update for SP or CMM Procedure
Web	1. Click Maintenance > Firmware Upgrade. 2. Click the button for Enter Firmware Upgrade Mode, then click OK in the upgrade confirmation dialog box to proceed. The Firmware Upgrade page displays the property for uploading the firmware image. Note – If the firmware image has not been downloaded from the Oracle product download web site, see these instructions to download the updated image: “Oracle ILOM Firmware Versions and Download Methods” in Oracle ILOM Feature Updates and Release Notes Firmware Release 4.0.x. 3. In the Firmware Upgrade page, perform one the following actions: Click Browse to specify the firmware image to upload, then click the Upload button. - or - Input a URL to upload the firmware image, then click the Upload button. Oracle ILOM validates the firmware image and then displays options in the Firmware Verification page. 4. In the Firmware Verification page, enable the applicable options: Preserve Configuration – Enable this option to save and restore the existing Oracle ILOM firmware settings after the firmware update is complete. For further details about this option, see “Preserve Oracle ILOM Configuration ” on page 294. Preserve BIOS Configuration (x86 server SPs only) - Enable this option to save and restore existing BIOS configurations after the update process is complete. This option is not supported on all x86 servers.

Oracle ILOM Interface	To Start and Run Firmware Update for SP or CMM Procedure
	Therefore, if this option is not presented, Oracle ILOM restores the default BIOS settings after completing the upgrade process. Delay BIOS Upgrade (x86 server SPs only) – Enable this option to postpone the x86 BIOS upgrade until after the next time the system is power-cycled. - Click Start to start the update process. - Click OK to proceed through a series of prompts until the Update Status page appears. - The system will either reboot or power-off when the Update Status indicates 100%. If your system powers off, refer to the documentation provided with your system for instructions on how to power on the system. Note - (x86 server SPs only) If you the server has a pending BIOS upgrade, the power reset could take longer to complete. This is expected behavior, as it is necessary to power cycle the server to upgrade the BIOS firmware. If the upgrade includes an FPGA update, the process can take as long as 26 minutes to complete.
CLI	- To load the Oracle ILOM firmware image using the CLI, issue the <code>load -source</code> command followed by the path to locate the firmware image you want to install. For example: <pre>load -source protocol://username:password@server_ip/<path_to_image>/<image.pkg></pre> Where the <i>protocol</i> can be: <i>http, https, ftp, tftp, sftp, scp</i> A series of prompts appear. - Type y to load the image file, then type y to enable the applicable options: Preserve Configuration – Enable this option to save and restore the existing Oracle ILOM firmware settings after the firmware update is complete. For further details about this option, see “Preserve Oracle ILOM Configuration” on page 294. Preserve BIOS Configuration (x86 server SPs only) - Enable this option to save and restore existing BIOS configurations after the update process is complete. This option is not supported on all x86 servers. Therefore, if this option is not presented, Oracle ILOM restores the default BIOS settings after completing the upgrade process. Delay BIOS Upgrade (x86 server SPs only) – Enable this option to postpone the x86 BIOS upgrade until after the next time the system is power-cycled. Note. All firmware update options presented for your server are enabled (y) by default when using a script (-script) to perform the firmware update. - Oracle ILOM displays a status message when the firmware process is complete. The system will either reboot or power-off to apply the new firmware image. If the system powers off, refer to the documentation provided with your system for instructions on how to power on the system. Note - (x86 server SPs only) If the server has a pending BIOS upgrade, the power reset could take longer to complete. This is expected behavior, as it is necessary to power cycle the server to upgrade the BIOS firmware. If the upgrade includes an FPGA update, the process can take as long as 26 minutes to complete.

2. To verify that the updated firmware version is installed, perform one of the following:

■ Web:

Log in to Oracle ILOM and click System Information > Firmware to view the firmware version installed.

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

■ **CLI:**

Type: `show /System/Firmware`

Related Information:

- [“Recover From a Network Failure During Firmware Update” on page 301](#)
- [Table 14, “File Transfer Methods,” on page 50](#)
- [“Oracle ILOM Firmware Versions and Download Methods” in *Oracle ILOM Feature Updates and Release Notes Firmware Release 4.0.x*](#)
- [Firmware Downloads and Release History for Oracle Systems \(http://www.oracle.com/technetwork/systems/patches/firmware/release-history-jsp-138416.html\)](http://www.oracle.com/technetwork/systems/patches/firmware/release-history-jsp-138416.html)
- [Firmware Resources \(http://www.oracle.com/technetwork/systems/patches/firmware/firmware-resources-1429462.html\)](http://www.oracle.com/technetwork/systems/patches/firmware/firmware-resources-1429462.html)

▼ Update Blade Chassis Component Firmware Images

The Oracle ILOM CMM provides a centralized user interface for managing firmware updates for the following upgradable blade chassis components:

- Storage blade servers
- CPU blade servers
- NEMs containing SPs

System administrators can choose to use the CMM web interface or the CLI to view chassis component firmware versions or initiate chassis component firmware updates.

The following procedure explains the process for updating a chassis component firmware image using the web interface Firmware Update page and the CLI chassis component targets for loading the firmware update.

Before You Begin

- Ensure that the initial firmware update requirements have been met. See [“Before You Begin the Firmware Update” on page 295](#).
- The firmware update process takes several minutes to complete. During this time, do not perform any other Oracle ILOM tasks. When the firmware update completes, the system component will either reboot or power off.

To start the firmware update process and to verify the update process completed successfully, follow these steps:

1. **To start the firmware update process for a server SP or CMM image, perform one of the following Oracle ILOM interface procedures:**

Oracle ILOM Interface	To start and run firmware update for blade chassis component (blades or NEMS) Procedure
Web	1. In the CMM web interface, click Firmware. 2. In the table, click the radio button adjacent to the chassis component for which you want to upgrade the firmware, then click the Firmware Update option in the Actions list box. The Firmware Upgrade page displays the property for uploading the firmware image. 3. In the Firmware Upgrade page, perform one the following actions: Click Browse to specify the firmware image to upload, then click the Upload button. - or - Input a URL to upload the firmware image, then click the Upload button. Oracle ILOM validates the firmware image, and then depending on the chassis component, Oracle ILOM either displays a button to start the firmware update process or displays a choice of configuration options for CPU blade server SPs. If you are updating the firmware for a CPU blade server SP proceed to step 4, otherwise proceed to step 5. 4. (CPU blade update only) In the Firmware Verification page, enable the applicable options available for CPU blade servers: Preserve Configuration – Enable this option to save and restore the existing Oracle ILOM firmware settings after the firmware update is complete. For further details about this option, see “Preserve Oracle ILOM Configuration ” on page 294. Preserve BIOS Configuration (x86 server SPs only) - Enable this option to save and restore existing BIOS configurations after the update process is complete. This option is not supported on all x86 servers. Therefore, if this option is not presented, Oracle ILOM restores the default BIOS settings after completing the upgrade process. Delay BIOS Upgrade (x86 server SPs only) – Enable this option to postpone the x86 BIOS upgrade until after the next time the system is power-cycled. 5. Click Start to start the update process. 6. Click OK to proceed through a series of prompts until the Update Status page appears. 7. The system will either reboot or power-off when the Update Status reaches 100%. If your system powers-off, refer to the documentation provided with your system for instructions about powering on the system component.

Oracle ILOM Interface	To start and run firmware update for blade chassis component (blades or NEMS) Procedure
	Note - (x86 server SPs only) If the server has a pending BIOS upgrade, the power reset could take longer to complete. This is expected behavior, as it is necessary to power cycle the server to upgrade the BIOS firmware. If the upgrade includes an FPGA update, the process can take as long as 26 minutes to complete.
CLI	1. Navigate to the blade or NEM Firmware target, for example: cd /System/Firmware/Other_Firmware/Firmware_# <i>Where Firmware_# is the number assigned to the specific blade server or NEM.</i> 2. To load the Oracle ILOM firmware image using the CLI, issue the <code>load -source</code> command followed by a path to locate the firmware image that you want to install. For example: load -source protocol://username:password@server_ip/<path_to_image>/<image.pkg> <i>Where the protocol can be: http, https, ftp, tftp, sftp, scp.</i> A message appears prompting you to load the image. 3. Type y to load the image file. Proceed to Step 4 for CPU blade firmware updates, otherwise proceed to Step 5 for storage blade or NEM firmware updates. 4. (CPU blade update only) Type y to enable the applicable update options such as: preserve SP configuration, preserve x86 BIOS settings, or delay x86 BIOS update Note – Not all x86 server SPs support the option to preserve the BIOS configuration settings. If the x86 BIOS option is not presented, Oracle ILOM will automatically preserve the default BIOS settings. For further information about the preserve SP configuration, see “Preserve Oracle ILOM Configuration” on page 294. 5. Oracle ILOM displays a status message when the firmware process is complete. The chassis component will either reboot or power off to apply the new firmware image. If your system powers-off, refer to the documentation provided with your system for instructions about powering on the system component. Note - (x86 server SPs only) If the server has a pending BIOS upgrade, the power reset could take longer to complete. This is expected behavior, as it is necessary to power cycle the server to upgrade the BIOS firmware. If the upgrade includes an FPGA update, the process can take as long as 26 minutes to complete.

2. To verify that the updated firmware version is installed, perform one of the following:

■ Web:

Log in to the Oracle ILOM CMM and click the System Information > Firmware to view the firmware version installed for each upgradable chassis component.

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

- **CLI:**
Type: `show /System/Firmware/Other_Firmware/Firmware_n`

Related Information:

- “Recover From a Network Failure During Firmware Update” on page 301
- Table 14, “ File Transfer Methods ,” on page 50
- “Oracle ILOM Firmware Versions and Download Methods” in *Oracle ILOM Feature Updates and Release Notes Firmware Release 4.0.x*
- Firmware Downloads and Release History for Oracle Systems (<http://www.oracle.com/technetwork/systems/patches/firmware/release-history-jsp-138416.html>)
- Firmware Resources (<http://www.oracle.com/technetwork/systems/patches/firmware/firmware-resources-1429462.html>)

▼ Recover From a Network Failure During Firmware Update

If a network failure occurs while performing a firmware update, Oracle ILOM automatically times out the session and reboots the system. After the system reboots, follow these guidelines to recover the firmware update process.

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

Reset Power to Service Processor or Chassis Monitoring Module

On occasion the blade chassis monitoring module (CMM) or the service processor (SP) for a server or a network express module (NEM) needs to be reset to complete an upgrade, or to clear an error state. The SP and CMM reset operation is similar to resetting a PC where all active processes are terminated and the system reboots.

Resetting the power on a server SP or CMM will automatically disconnect any current Oracle ILOM sessions and render the service processor unmanageable until the reset process is

complete. However, the host operating system on a server is not affected when a rackmount server SP or a CPU blade server SP is reset.

System administrators can reset the server SP, NEM SP, and the CMM from the web interface or the CLI. For further SP and CMM reset instructions, see the following procedure.

▼ Reset Power to Server SP, NEM SP, or CMM

Before You Begin

- Host Control and Reset (r) role is required to reset a SP or CMM.
- After clicking the web Reset button or issuing the CLI reset command, Oracle ILOM will automatically display a prompt to confirm the reset operation, unless a CLI -script option is specified (**reset** *[options]* *target*).

This procedure provides both web and CLI instructions.

- To reset the power to an SP or CMM, perform one of the following:

Oracle ILOM Interface	Reset Power to SP or CMM
Web	Perform one of the following: ■ Server SP: Click ILOM Administration > Maintenance > Reset SP, then click the Reset SP button. ■ CMM and blade chassis components: Click ILOM Administration > Maintenance >Reset Components. Click the radio button adjacent to the chassis component (CMM, blade, NEM), then click the Reset button.
CLI	Perform one of the following: ■ Server SP: To reset the server SP, type: reset /SP ■ CMM blade chassis components: To reset the CMM, type: reset /CMM To reset a blade SP, type: reset /Servers/Blades/BLn/SP To reset a NEM SP, type: reset /System/IO_Modules/NEMn/SP

Managing ASR Component States

In Oracle ILOM you can enable or disable the requested state for Automatic System Recovery (ASR) components, such as, processors and memory modules.

Disabling ASR components in Oracle ILOM is done when you want to remove resources from the available resource list. For example, you might disable an ASR component when you replace a component or remove it from the server. After you disable an ASR component in Oracle ILOM, the component becomes non-operational and is no longer eligible for booting. Enabling a disabled ASR component in Oracle ILOM is done when you are ready to make the ASR component operational and eligible for booting.

▼ Manually Enable or Disable an ASR Component

Before You Begin

- The Oracle ILOM property for requested state is available only on Oracle servers that are equipped with ASR supported components.
- To modify the Oracle ILOM property for requested state you must have Admin (a) role privileges enabled.
- Both the Oracle ILOM CLI and web interface support properties for viewing or modifying the requested state of an ASR component.

1. **To view the requested state of an ASR component, perform the instructions below for your preferred Oracle ILOM interface:**

Oracle ILOM Interface	View the requested state of an ASR component.
Web	1. Navigate to the ASR component in the Oracle ILOM web interface. For example, for Oracle servers equipped with ASR supported processors, click System Information > Processors. 2. In the component page, view the requested state column shown in the table for the component.
CLI	■ Use the show command to view the requested state of an ASR component. For example, to view the requested state for a CPU, you could type: show /System/Processors/CPUs/CPU_1 The requested_state for the CPU_1 appears.

2. **To disable or enable the requested state of an ASR component, perform the instructions below for your preferred Oracle ILOM interface:**

Oracle ILOM Interface	Disable or enable the component state for an ASR component.
Web	1. Navigate to the ASR component in the Oracle ILOM web interface. For example, for Oracle servers equipped with ASR supported processors, click System Information > Processors. 2. In the component page, select a component from the table and click Delete or Enable in the Actions list box. A confirmation message appears, click OK to continue or click Cancel to cancel the operation. If you modified the requested state while the host is powered off, the modification will take effect the next time the host is powered on. If you modified the requested state while the host is powered on, the modification will take effect the next time the host is power cycled.
CLI	■ Use the set command to modify the requested state of an ASR component. For example, to modify the requested state of a ASR processor such as CPU_1, you could type: set /System/Processors/CPUs/CPU_1 requested_state=disabled enabled A confirmation message appears, click Y to continue or click N to cancel the operation. If you modified the requested state while the host is powered off, the modification will take effect the next time the host is powered on. If you modified the requested state while the host is powered on, the modification will take effect the next time the host is power cycled.

Related Information:

- For ASR feature details that might be specific for your Oracle server, see the administration guide provided with the server.

Managing Active and Standby SP Redundancy Roles (SPARC)

For Oracle's SPARC servers populated with two service processors (SPs), Oracle ILOM provides properties for managing the active and standby roles associated with the SPs. For instance, in the Oracle ILOM web interface or CLI, you can gracefully or forcibly initiate a failover action that will cause the roles of the active SP and standby SP to change. You can also view the redundancy status assigned to each SP.

Note - The **Force Failover** (true) option in Oracle ILOM should only be used when you are instructed to do so by qualified Oracle service personnel. System Administrators, when necessary, should always use the **Graceful Failover** (grace) option in Oracle ILOM to gracefully negotiate the redundancy role change for the active and standby SPs.

For instructions on how to view the redundancy status of an SP or modify the SP roles, see the following procedure.

▼ Modify Active and Standby SP Redundancy Roles (SPARC)

Before You Begin

- The Oracle ILOM redundancy properties for active and standby SPs are available only on Oracle's SPARC servers that are equipped with two SPs.
- To modify the Oracle ILOM redundancy properties on an active or standby SP you must have Admin (a) role privileges enabled.
- Both the Oracle ILOM web interface and CLI support viewing or modifying the redundancy properties on a redundant SP system.

1. To view the redundancy status assigned to an SP, perform the instructions below for your preferred Oracle ILOM interface:

Oracle ILOM Interface	View the assigned redundancy status.
Web	1. Log in to the active server SP on the redundant Oracle SPARC system. Note – If the active server SP is unresponsive, log in to the standby SP. The Redundancy properties for the standby SP appear in the Oracle ILOM interface only when the active SP becomes unresponsive. 2. Click ILOM Administration > Maintenance > Redundancy. 3. View the Redundancy Status property. See “SP Redundancy Status Descriptions” on page 306.
CLI	1. Log in to the active server SP on the redundant Oracle SPARC system. Note – If the active server SP is unresponsive, log in to the standby SP. The Redundancy properties for the standby SP appear in the Oracle ILOM interface only when the active SP becomes unresponsive. 2. Type: show /SP/redundancy See “SP Redundancy Status Descriptions” on page 306.

2. To modify the active SP and standby SP roles, perform the instructions below for your preferred Oracle ILOM interface:

Oracle ILOM Interface	Modify the roles of the active and standby SPs.
Web	■ In the (ILOM Administration > Maintenance >) Redundancy Settings page, perform one of the following failover actions:

Oracle ILOM Interface	Modify the roles of the active and standby SPs. Graceful Failover (Recommended Action) — To gracefully negotiate the role change in a redundant SP system, set Graceful as the Failover action and click either the Promote or Demote button. Force Failover (Oracle Service Action) — To forcibly change the roles in a redundant SP system, set Force as the Failover action and click either the Promote or Demote button. Note - The Promote button is shown when the SP is currently the standby SP. The Demote button is shown when the SP is currently the active SP.
CLI	1. Type the following to navigate to the redundancy target: cd /SP/redundancy 2. To set the failover action for the managed SP, type: set initiate_failover_action=true force <i>true (Recommended Action)</i> — To gracefully negotiate the role change in a redundant SP system, set true as the Failover action. <i>force (Oracle Service Action)</i> — To forcibly change the roles in a redundant SP system, set force as the Failover action.

SP Redundancy Status Descriptions

Status	Description
Active	An Active status appears when the selected SP is the active SP.
Standby	A Standby status appears when the selected SP is the standby SP.
Standalone	A Standalone status appears to indicate when the other SP is not responsive.

Backing Up, Restoring, or Resetting the Oracle ILOM Configuration

The Backup and Restore properties provided in Oracle ILOM enable system administrators to copy the current Oracle ILOM configuration to a backup XML file, and restore the configuration when needed. System administrators can choose to use the backup XML configuration file to restore the settings on the present SP or CMM, or use the backup file to install the configuration settings on other CMMs or server SPs.

The Reset Default properties provided in Oracle ILOM enable system administrators to clear any user-set Oracle ILOM configuration properties and restore them to their factory default values.

System administrators can back up and restore the Oracle ILOM configuration, and reset the configuration settings to defaults from the web interface or CLI. For further information about the use of the Oracle ILOM back up, restore, or reset default features, see the following topics:

- [“Using Backup, Restore, and Reset Default Operations” on page 307](#)
- [“User Role Required for Backing Up or Restoring the Oracle ILOM Configuration” on page 308](#)
- [“Back Up the Oracle ILOM Configuration Settings” on page 308](#)
- [“Optionally Edit the Oracle ILOM Backup XML Configuration File ” on page 310](#)
- [“Restore the Oracle ILOM Backup XML File” on page 313](#)
- [“Reset the Oracle ILOM Configuration to Factory Defaults” on page 315](#)

Using Backup, Restore, and Reset Default Operations

System administrators can use the operations for Backup, Restore, and Reset Defaults in the following ways:

1. **Replicate the Oracle ILOM configuration for use on other systems.**

System administrators can replicate the Oracle ILOM configuration for use on other Oracle server SPs or CMMs by following these steps:

- a. Customize the Oracle ILOM configuration as needed
For example, define user accounts, modify default network settings, set alert notifications, define system policies, and so on.
- b. Save the Oracle ILOM configuration to a backup XML file.
- c. Edit the backup XML file to remove settings that are unique to a particular system (such as IP address).
- d. Perform a restore operation to replicate the configuration onto the other Oracle server SPs or CMMs.

2. **Recover a working Oracle ILOM configuration when the existing Oracle ILOM configuration is no longer working.**

If modifications were made to the Oracle ILOM configuration since the last backup operation and the current Oracle ILOM configuration is no longer working, system administrators can recover the working backup configuration by following these steps:

- a. Reset the Oracle ILOM configuration to defaults.
- b. Restore the Oracle ILOM configuration to the last known working configuration.

User Role Required for Backing Up or Restoring the Oracle ILOM Configuration

Firmware Release	User Role Required	Related information
■ Early releases of Oracle ILOM firmware version 3.2.6.x ■ All 3.2.5.x and preceding releases of Oracle ILOM firmware versions.	Any user role can back up the Oracle ILOM configuration properties. When you restore properties from a backed up configuration, only the properties in which you have privileges to change are restored to the SP or CMM. At a minimum, the Admin (a) role is required to initiate the Restore operation.	■ Table 10, “Privileges Granted by a User Profile,” on page 44 Privileges Granted by a User Profile ■ Table 11, “Privileges Granted by Individual User Roles,” on page 45 Privileges Granted by Individual User Roles ■ “Configuring Local User Accounts ” on page 51
■ Later releases of Oracle ILOM firmware version 3.2.6.x and all subsequent firmware versions that follow.	At a minimum, the Admin (a) role is required to initiate a back up or restore operation of the Oracle ILOM configuration. Only the configuration properties in which you have privileges to change are either backed up or restored to the SP or CMM.	

▼ Back Up the Oracle ILOM Configuration Settings

System administrators can save a backup copy of the Oracle ILOM configuration file that is actively running on the server SP or CMM. Upon initiating a Backup operation, all Oracle ILOM client sessions to the SP or the CMM are momentarily suspended. The suspended sessions resume to normal after the Backup operation is complete. A Backup operation typically takes two to three minutes to complete.

The following Oracle ILOM configuration backup procedure provides both web and CLI instructions for the SP and the CMM.

- **To back up the Oracle ILOM configuration to an XML file, perform the following steps for one of the Oracle ILOM user interfaces listed.**

Oracle ILOM User Interface	Backing Up Oracle ILOM Configuration Settings to XML File
Web	1. Click ILOM Administration > Configuration Management > Backup/Restore. 2. Click Backup in the Operations box. 3. (Optional) Select the Include Fault Data check box. When selected, the backup operation will include all fault data incidents in the backup copy of the xml configuration file.

Oracle ILOM User Interface	Backing Up Oracle ILOM Configuration Settings to XML File
	The Include Fault Data check box is available for configuration as of Oracle ILOM firmware 3.2.6. Note – A passphrase must be provided to back up fault data for all incidents. For further details about entering a passphrase, see Step 5 below. - Click the Transfer Method box to specify a method for transferring the Oracle ILOM configuration file. For property descriptions of each file transfer method, see Table 14, “ File Transfer Methods ,” on page 50. - To encrypt the backup configuration file, type a passphrase in the Passphrase text box, and then retype the passphrase in the Confirm Passphrase text box. The backup file is encrypted using the passphrase specified. Note – To back up sensitive data such as passwords, SSH keys, certificates, LDoms and so forth, you must specify a passphrase. The passphrase length must be a minimum of 16 characters. - Click Run to initiate the Backup operation. When the Backup operation is executing, client sessions to the Oracle ILOM SP or the CMM are momentarily suspended. The sessions will resume to normal after the Backup operation is complete.
CLI	- Navigate to the config CLI target, for example: <pre>cd /SP/config cd /CMM/config</pre> (Optional) To include fault data for all incidents in the backup operation, set the property value for <code>include_faultdata</code> to <code>true</code>. For instance: <pre>set include_faultdata=true</pre> The <code>include_faultdata</code> property is available for configuration as of Oracle ILOM firmware version 3.2.6. Note – A passphrase must be provided to back up fault data in the xml configuration file. For further details about entering a passphrase, see Step 3 below. - To encrypt the backup configuration file, set the a value for the passphrase property, for example: <pre>set passphrase=value</pre> The backup file is encrypted using the passphrase specified. Note – To back up sensitive data such as passwords, SSH keys, certificates, LDoms and so forth, you must specify a passphrase. The passphrase length must be a minimum of 16 characters. - To initiate the Backup operation, type the following command from within the <code>/SP/config</code> or <code>/CMM/config</code> directory. For example: <pre>set dump_uri=transfer_method://username:password@ipaddress_or_hostname/directorypath/filename</pre> Where the <i>transfer method</i> can be: <code>ftp</code>, <code>ftp</code>, <code>sftp</code>, <code>scp</code>, <code>http</code>, or <code>https</code> For property descriptions of each file transfer method, see Table 14, “ File Transfer Methods ,” on page 50. For example: <pre>set dump_uri=scp://adminuser:userpswd@1.2.3.4/Backup/Lab9/SP123.config</pre> When the Backup operation is executing, client sessions to the Oracle ILOM SP or the CMM are momentarily suspended. The sessions will resume to normal after the Backup operation is complete.

Related Information:

- [“Optionally Edit the Oracle ILOM Backup XML Configuration File ” on page 310](#)
- [“Restore the Oracle ILOM Backup XML File” on page 313](#)
- [“Using Backup, Restore, and Reset Default Operations” on page 307](#)
- [“Managing Oracle ILOM Log Entries” in *Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*](#)

▼ Optionally Edit the Oracle ILOM Backup XML Configuration File

Advanced users can use the backup XML file to provision other Oracle server SPs or CMMs on the network with the same Oracle ILOM configuration. Prior to using a backup XML file on another system, system administrators should edit the file to remove any information that is unique to a particular system (for example, IP address).

Example XML File:

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

```
<SP_config version="3.0">
<entry>
<entry>
<property>/SP/clock/datetime</property>
<value>Mon May 12 15:31:09 2010</value>
</entry>
. . .
<property>/SP/check_physical_presence</property>
<entry>
<property>/SP/config/passphrase</property>
<value encrypted="true">89541176be7c</value>
</entry>
. . .
<value>>false</value>
<entry>
<property>/SP/network/pendingipaddress</property>
<value>1.2.3.4</value>
</entry>
. . .
</entry>
<entry>
```

```

<property>/SP/network/commitpending</property>
<value>true</value>
</entry>
. . .
<entry>
<entry>
<property>/SP/services/snmp/sets</property>
<value>enabled</value>
</entry>
. . .
<property>/SP/hostname</property>
<entry>
<property>/SP/users/john/role</property>
<value>aucro</value>
</entry>
<entry>
<property>/SP/users/john/password</property>
<value encrypted="true">c21f5a3df51db69fdf</value>
</entry>
</SP_config>
<value>labysystem12</value>
</entry>
<entry>
<property>/SP/system_identifier</property>
<value>SUN BLADE X8400 SERVER MODULE, ILOM v3.0.0.0, r32722</value>
</entry>
. . .

```

1. Consider the following in the example XML file:

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

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

For example:

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

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

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

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

- **To change a password, delete the encrypted="true" setting and the encrypted password string and type in the new password. For example, to change the password for the user john, modify the XML file as follows:**

Change:

```
<entry>
<property>/SP/users/john/password</property>
<value encrypted="true">c21f5a3df51db69fdf</value>
</entry>
```

To:

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

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

Related Topics

- [“Optionally Edit the Oracle ILOM Backup XML Configuration File ” on page 310](#)
- [“Restore the Oracle ILOM Backup XML File” on page 313](#)

- [“Using Backup, Restore, and Reset Default Operations” on page 307](#)

▼ **Restore the Oracle ILOM Backup XML File**

System administrators can perform a Restore operation to retrieve the XML file from a remote system, parse the contents, and update the SP (or CMM) with the backed-up configuration data. Upon initiating a Restore operation, all Oracle ILOM client sessions to the restoring server SP or CMM are momentarily suspended. The suspended sessions resume to normal after the Restore operation completes. A Restore operation typically takes two to three minutes to complete.

Before You Begin

- To perform a configuration restore operation in Oracle ILOM, the Administrator (administrator) profile role is required or the following user roles must be assigned: Admin (a), User Management (u), Console (c) Reset and Host Control (r) and Read Only (o).
For further details, see [“User Role Required for Backing Up or Restoring the Oracle ILOM Configuration ” on page 308](#).
- Sensitive data in the backup file taken from Oracle ILOM firmware 3.2.1+ versions can not be restored to an Oracle system running firmware prior to Oracle ILOM 3.2.1.

The following Oracle ILOM configuration restore procedure provides both web and CLI instructions for the SP and the CMM.

- **To restore the backed up Oracle ILOM configuration XML file, perform the following steps for one of the Oracle ILOM user interfaces listed.**

Oracle ILOM User Interface	Restoring a Backup Copy of the Oracle ILOM Configuration Settings
Web	1. Click ILOM Administration > Configuration Management > Backup/Restore. 2. Click Restore in the Operations box. 3. (Optional) Select the Include Fault Data check box. When selected, the restore operation will include all fault data incidents in the restored xml configuration file. The Include Fault Data check box is available for configuration as of Oracle ILOM firmware 3.2.6. Note – A passphrase must be provided to restore fault data. For further details about entering a passphrase, see Step 5 below. 4. Click the Transfer Method box to specify a method for transferring the Oracle ILOM configuration file. For property descriptions of each file transfer method, see Table 14, “ File Transfer Methods ,” on page 50. 5. If the backup configuration file was encrypted with a passphrase, type the passphrase in the Passphrase text box, and then retype the passphrase in the Confirm Passphrase text box.

Oracle ILOM User Interface	Restoring a Backup Copy of the Oracle ILOM Configuration Settings
	Note – The passphrase entered must match the passphrase used to encrypt the backup configuration file. The passphrase length must be a minimum of 16 characters. 6. Click Run to initiate the Restore operation. When the Restore operation is executing, client sessions to the Oracle ILOM SP or the CMM are momentarily suspended. The sessions will resume to normal after the Restore operation is complete.
CLI	1. Navigate to the config CLI target, for example: <pre>cd /SP/config</pre> <pre>cd /CMM/config</pre> 2. (Optional) To restore previously backed up fault data in the xml configuration file, set the property value for <code>include_faultdata</code> to <code>true</code>. For instance: <pre>set include_faultdata=true</pre> The <code>include_faultdata</code> property is available for configuration as of Oracle ILOM firmware version 3.2.6. Note – A passphrase must be provided to restore fault data in the xml configuration file. For further details about entering a passphrase, see Step 3 below. 3. If the backup configuration file was encrypted with a passphrase, set the value for the passphrase property to the passphrase used to encrypt the file, for example: <pre>set passphrase=value</pre> Note – The passphrase entered must match the passphrase used to encrypt the backup configuration file. The passphrase length must be a minimum of 16 characters. 4. To initiate the Restore operation, type the following command from within the <code>/SP/config</code> or <code>/CMM/config</code> directory. For example: <pre>set load_uri=transfer_method://username:password@ipaddress_or_hostname/ directorypath/filename</pre> Where the <i>transfer method</i> can be: tftp, ftp, sftp, scp, http, or https. For property descriptions of each file transfer method, see Table 14, “File Transfer Methods,” on page 50. For example: <pre>set load_uri=scp://adminuser:userpswd@198.51.100.4/Backup/Lab9/SP123.config</pre> When the Restore operation is executing, client sessions to the Oracle ILOM SP or the CMM are momentarily suspended. The sessions will resume to normal after the Restore operation is complete.

Related Information:

- [“Using Backup, Restore, and Reset Default Operations” on page 307](#)
- [“Restore the Oracle ILOM Backup XML File” on page 313](#)
- [“User Role Required for Backing Up or Restoring the Oracle ILOM Configuration” on page 308](#)

▼ Reset the Oracle ILOM Configuration to Factory Defaults

System administrators can restore the current Oracle ILOM configuration settings on the SP or the CMM to the original factory default settings.

For a description of the possible values you can set for a Reset to Defaults operation, see the following table.

Reset Property Value	Description
All	Set the All option to reset all of the Oracle ILOM configuration data to the default settings at the next service processor reset. This action does not erase the log file entries.
Factory	Set the Factory option to reset all of the Oracle ILOM configuration data to the default settings and erase all log files at the next service processor reset.
None (default)	Set the None option for normal operation while using the current configurations. Or use the None option to cancel a pending Reset to Defaults operation (All or Factory) before the next service processor reset.

- To perform a Reset to Defaults operation on a server SP or CMM, perform the following steps for one of the Oracle ILOM user interfaces listed.

Oracle ILOM Interface	Reset to Defaults Operation for SP or CMM
Web	1. Click ILOM Administration > Configuration Management > Reset Defaults. 2. Click the Reset Defaults list box to specify one of the following values: <i>None</i>, <i>All</i> or <i>Factory</i>. 3. Click the Reset Defaults button.
CLI	Perform one of the following: ■ Server SP: Type: <code>set /SP reset_to_defaults=all none factory</code> ■ CMM: Type: <code>set /CMM reset_to_defaults=all none factory</code>

Related Information:

- [“Reset Power to Service Processor or Chassis Monitoring Module ” on page 301](#)

Maintaining x86 BIOS Configuration Parameters

Description	Links
Refer to this topic to identify ways you can manage the x86 BIOS configuration.	■ “BIOS Configuration Management” on page 317
Refer to these topics for information about Oracle ILOM BIOS configuration features, terminology, and properties.	■ “Oracle ILOM: BIOS Configuration Features” on page 318 ■ “Oracle ILOM: BIOS Terminology” on page 319 ■ “Web and CLI: BIOS Properties” on page 319
Refer to this section for information describing how to perform BIOS configuration tasks from Oracle ILOM.	■ “Performing BIOS Configuration Tasks From Oracle ILOM” on page 323

Related Information

- Administration guide for Oracle x86 server, Oracle System Assistant
- Administration guide for Oracle x86 server, BIOS Setup Utility

BIOS Configuration Management

The BIOS configuration parameters on an Oracle x86 server are manageable from the host BIOS Setup, the Oracle System Assistant interface, and the Oracle ILOM CLI and web interface. The following topics in this section describe how to manage the BIOS configuration from the Oracle ILOM interfaces.

- [“Oracle ILOM: BIOS Configuration Features” on page 318](#)
- [“Oracle ILOM: BIOS Special Considerations ” on page 318](#)
- [“Oracle ILOM: BIOS Terminology” on page 319](#)
- [“Web and CLI: BIOS Properties” on page 319](#)

Note - For instructions on how to manage the BIOS configuration from the host BIOS Setup or from the Oracle System Assistant, refer to the Oracle x86 server administration guide.

Oracle ILOM: BIOS Configuration Features

Oracle ILOM provides a set of configurable properties that help you to manage the BIOS configuration parameters on an Oracle ILOM managed x86 server. These configurable Oracle ILOM properties enable you to:

- Back up a copy of the configuration parameters in the BIOS non-volatile data store.
- Restore a copy of the backed-up configuration parameters to the BIOS non-volatile data store.
- Reset the parameters in the BIOS non-volatile data store to factory defaults.

In addition, Oracle ILOM dynamically monitors the parameters in the BIOS non-volatile data store to ensure that they are in sync with the parameters in the Oracle ILOM BIOS Configuration file. A configuration sync status, appearing in the CLI and web interface, indicates the current state of the BIOS parameters stored in the Oracle ILOM BIOS Configuration file.

Note - For advanced users who need to provision the BIOS configuration to another Oracle x86 server, see [“Optionally Edit the Oracle ILOM Backup XML Configuration File ” on page 310.](#)

Oracle ILOM: BIOS Special Considerations

- The Oracle ILOM BIOS configuration might increase host boot times when the Oracle ILOM BIOS configuration file is out of sync with the host BIOS non-volatile data store.
- Updating the Oracle ILOM firmware on the server SP can affect the Oracle ILOM BIOS configuration parameters when the option for “Preserve existing BIOS configuration” is enabled. For more details about performing a firmware update and preserving the BIOS configuration parameters maintained by Oracle ILOM, see [“Updating Oracle ILOM Firmware” on page 293.](#)

Oracle ILOM: BIOS Terminology

Oracle ILOM Term	Description
BIOS	The BIOS on an Oracle x86 server is the boot firmware program that controls the system from the time the host server powers on to when the operating system takes over. The BIOS stores the system's date, time, and configuration information in a battery-powered, non-volatile data store.
BIOS version	A read-only property indicating the current BIOS firmware version installed on an Oracle x86 server.
BIOS non-volatile data store	The Oracle x86 server BIOS configuration parameters that are currently stored on the non-volatile memory chip.
Oracle ILOM BIOS configuration file	A dynamically maintained XML file on the server SP that contains a list of the BIOS configuration parameters that were last retrieved from the BIOS non-volatile data store.
Backup BIOS configuration	The configurable properties in Oracle ILOM that enable you to retrieve a copy of the parameters currently set in the BIOS non-volatile data store and save them to the Oracle ILOM BIOS Configuration file on the server SP.
Restore BIOS configuration	Configurable properties in Oracle ILOM that enable you to export the parameters in the Oracle ILOM BIOS Configuration file to the BIOS non-volatile data store.
BIOS configuration parameters	Typically the BIOS configuration parameters that are copied or exported by Oracle ILOM include the values for: setup, boot list, and boot devices.

Web and CLI: BIOS Properties

- [Table 90, “BIOS Web Navigation and CLI Targets,” on page 319](#) BIOS Web Navigation and CLI Targets
- [Table 91, “BIOS Web and CLI Properties,” on page 319](#) BIOS Web and CLI Properties
- [Table 92, “-force Option for CLI Commands: load and dump,” on page 322](#) -force Option for CLI Commands: load and dump

TABLE 90 BIOS Web Navigation and CLI Targets

Web Navigation	CLI Targets
System Management > BIOS	/System/BIOS
	/System/BIOS/Config

TABLE 91 BIOS Web and CLI Properties

Property Name	Type	Value(s)	Description
System BIOS Version (system_bios_version=)	Read-only		The system BIOS Version property identifies the version of the BIOS firmware that is currently installed on the managed Oracle x86 server.

Property Name	Type	Value(s)	Description
Boot Mode (boot_mode=)	Read-only	Legacy UEFI	The BIOS Boot Mode property indicates that the system boots in one of the following modes: ■ Legacy – The system boots in the traditional “PC-AT” boot environment. ■ UEFI – The system boots in a UEFI specification-compliant boot environment. To adjust the BIOS boot mode, refer to the administration guide for your system.
BIOS Configuration: Sync Status (config_sync_status=)	Read-only	OK Reboot Required Internal Error	Note - As of firmware 3.2.4, the BIOS Sync Status property is not available on all Oracle x86 servers. The BIOS Configuration Sync Status property indicates one of the following states: ■ OK – The BIOS configuration parameters maintained by Oracle ILOM are in-sync with the configuration parameters in the BIOS non-volatile data store. ■ Reboot Required – The BIOS configuration parameters maintained by Oracle ILOM are out-of-sync with the configuration parameters in the BIOS non-volatile data store. The Oracle x86 server must be rebooted to sync the BIOS parameters. ■ Internal Error – Oracle ILOM is unable to read the BIOS non-volatile data store and is prevented from initiating a BIOS Backup or Restore operation. For further assistance, contact Oracle Service.
BIOS Configuration: Reset To Defaults (reset_to_defaults=)	Read Write	Factory None	The Reset To Defaults property provides one of the following values: ■ Factory – Sets the configuration parameters in the BIOS non-volatile data store to factory defaults. ■ None – This value (None) appears after resetting the parameters in the BIOS non-volatile data store to factory defaults.
BIOS Configuration: Backup (dump_uri=)	Write-only		The BIOS Configuration Backup property enables you to create a copy of the parameters in the BIOS non-volatile data store and save those parameters to a BIOS Configuration file in the ILOM file system. For instructions for backing up the BIOS configuration, see “Back Up the BIOS Configuration” on page 327.

Property Name	Type	Value(s)	Description
BIOS Configuration: Restore Status (restore_status=)	Read-only	OK Restore pending Partial restore: invalid configuration entry Partial restore: invalid boot order entry Partial restore: invalid configuration and boot order entries	Note - As for firmware 3.2.4, the Restore Status property is not available on all Oracle x86 servers. The BIOS Configuration Restore Status property indicates one of the following states: ■ OK – The last Restore operation succeeded for restoring the Oracle ILOM BIOS configuration parameters to the host BIOS non-volatile data store. ■ Restore pending – The Restore operation is pending a host power off. Note – The Restore operation is performed by Oracle ILOM when the host server is powered off. ■ Partial restore: invalid configuration entry – The last Restore operation failed to restore one or more of the host BIOS configuration parameters. ■ Partial restore: invalid boot order entry – The last Restore operation failed to restore one or more boot devices in the host boot order list. ■ Partial restore: invalid configuration and boot order entries – The last Restore operation failed to restore one or more BIOS configuration parameters and one or more boot devices in the host boot order list.
BIOS Configuration: Restore (load_uri= restore_options)	Read Write	All Configuration only Bootlist only Cancel Restore	The BIOS Configuration Restore property enables you to restore the BIOS parameters previously saved by Oracle ILOM to the host BIOS non-volatile data store. The options for restoring the BIOS parameters include: ■ All – Restores all BIOS configuration parameters that were previously saved by Oracle ILOM. ■ Configuration only – Restores the previously saved setup parameters. ■ Bootlist only – Restores the host boot list parameters previously saved by Oracle ILOM. ■ Cancel Restore (or action=cancel) – Cancels the initiated Restore operation. Note - The Cancel Restore option in the web interface is only available if: (1) you initiated a Restore operation, and (2) the host operating system on the managed Oracle x86 server has not yet been powered down or reset. Note - As of firmware 3.2.4, the Cancel Restore option is not supported on all Oracle x86 servers. For instructions for restoring the BIOS configuration, see “Restore BIOS Configuration ” on page 328.

Property Name	Type	Value(s)	Description
Transfer Method Options	Read Write	Browser TFTP FTP SFTP SCP HTTP HTTPS	When importing or exporting the Oracle ILOM BIOS configuration parameters, you can specify one of the following transfer methods: ■ Browser – Web interface option only. This option enables you to specify the location of the file. ■ TFTP – This option enables you to specify the TFTP host IP address or name and the directory path to the file. ■ FTP – This option enables you to specify the host IP address or name, user name and password for the FTP server, as well as the directory path to the file location. ■ SFTP – This option enables you to specify the host IP address or name, username and password for the SFTP server, as well as the directory path to the file location. ■ SCP – This option enables you to specify the host network address, user name and password for the SCP server, as well as the directory path to the file location. ■ HTTP – This option enables you to specify the host network address, username and password for the HTTP server, as well as the directory path to the file location. ■ HTTPS – This option enables you to specify the host network IP address or name, user name and password for the HTTPS server, as well as the directory path to the file location.

TABLE 92 -force Option for CLI Commands: load and dump

load_uri=-force <i>restore_option/transfer_method://username:password@ipaddress_or_hostname /directorypath/filename</i>
dump_uri=-force <i>transfer_method://username:password@ipaddress_or_hostname /directorypath/filename</i>
Usage – You must specify the -force option to prevent the load or dump command from failing when: (1) a “Pending Restore” state appears for Restore Status (restore_status=pending_restore) or (2) when a “Reboot Needed” state appears for BIOS Configuration Sync (config_sync_status=reboot_needed).

Caution - An out-of-sync version of the host BIOS Configuration file is copied to the Oracle ILOM file system when: (1) a “Reboot Needed” state appears for BIOS Configuration Sync (`sync_status=reboot_needed`) and (2) the `dump_uri=-force` option is used to back up the BIOS Configuration file.

Caution - The parameters in an existing pending restore BIOS Configuration file are replaced with the parameters from the last Backup BIOS Configuration file when: (1) a “Restore Pending” state appears for Restore Status (`restore_status=restore_pending`) and (2) the `load_uri=-force` option is used to restore the parameters in the host BIOS non-volatile data store.

Performing BIOS Configuration Tasks From Oracle ILOM

- [“Requirements for BIOS Configuration Tasks” on page 323](#)
- [“View the BIOS Configuration Sync Status and Sync the Configuration Parameters” on page 324](#)
- [“Reset Factory Defaults for SP and Oracle ILOM BIOS” on page 326](#)
- [“Back Up the BIOS Configuration ” on page 327](#)
- [“Restore BIOS Configuration ” on page 328](#)

Requirements for BIOS Configuration Tasks

Prior to backing up or restoring the BIOS configuration parameters, the following requirements should be met:

- The following user roles are required in Oracle ILOM to sync, restore, or back up the BIOS configuration parameters:

BIOS Configuration Task	Oracle ILOM User Roles	Description:
Restore the BIOS configuration (<code>load_uri=</code>)	Reset and Host Control (r) Admin (a)	The Reset and Host Control (r) role and the Admin (a) role are required to load the configuration parameters in the host BIOS non-volatile data store. Note - Oracle ILOM replaces the parameters in the host BIOS non-volatile data store with the parameters that were last set in the Oracle ILOM BIOS Configuration file.
Back up the BIOS configuration (<code>dump_uri=</code>)	Reset and Host Control (r) Admin (a)	The Reset and Host Control (r) role and the Admin (a) role are both required to replace the configuration parameters in the Oracle ILOM Configuration file. Note - Oracle ILOM replaces the parameters in Oracle ILOM Configuration file with the parameters

BIOS Configuration Task	Oracle ILOM User Roles	Description:
		that were last set in the host BIOS non-volatile data store.
Sync BIOS configuration (reset /System or stop /System)	Admin (a)	The Admin (a) role is required to reset the power (or power off) on the managed Oracle x86 server.

- Review the [“Web and CLI: BIOS Properties” on page 319](#) prior to performing the BIOS configuration tasks that are documented in this section.
- If the managed Oracle x86 server is new, it should be powered-on to enable the host BIOS boot process to detect the boot devices, create an initial boot order, and save these parameters to the BIOS non-volatile data store. The managed Oracle x86 server should then be powered cycled to sync the BIOS non-volatile data store with the Oracle ILOM BIOS Configuration file.
- Setting factory defaults for the /SP or for the /System/BIOS can inadvertently affect one another. For example, setting the /SP/reset_to_defaults to *factory* might cause Oracle ILOM to lose the settings for /System/BIOS/reset_to_defaults. For instructions on how to set factory defaults for the SP and BIOS configuration, follow the steps described in [“Reset Factory Defaults for SP and Oracle ILOM BIOS” on page 326](#).

▼ View the BIOS Configuration Sync Status and Sync the Configuration Parameters

Before You Begin

- Review the [“Requirements for BIOS Configuration Tasks” on page 323](#).

Follow these steps to view the BIOS Configuration Sync Status and, if necessary, to sync the BIOS configuration parameters in the host non-volatile data store with the parameters in the Oracle ILOM BIOS Configuration file.

1. To view the state of the parameters currently in the Oracle ILOM BIOS Configuration file, perform one of the following:

- For the web interface, click System Management > BIOS
- For the CLI, type: **show /System/BIOS/Config**

An OK state indicates that the parameters in the Oracle ILOM BIOS Configuration file are in-sync with the BIOS non-volatile data store.

A `Reboot_Required` state indicates that the Oracle ILOM BIOS Configuration file is out-of-sync with the BIOS non-volatile data store.

An `Internal_Error` state indicates that Oracle ILOM is unable to read the BIOS non-volatile data store. This internal error prevents the BIOS Configuration Backup and Restore operations from being initiated in Oracle ILOM. For further assistance, contact Oracle Service.

2. To sync the parameters in the BIOS non-volatile data store with the Oracle ILOM BIOS Configuration file, perform one of the following actions to power-cycle the managed Oracle x86 server.

- From the web interface, click Host Management > Power Control > Power Cycle.
- From the CLI, type: `reset /System`

Oracle ILOM retrieves the parameters set in the BIOS non-volatile data store, saves them to the Oracle ILOM BIOS Configuration file, and updates the state for the Configuration Sync Status.

Related Information:

- [“Reset BIOS Configuration to Factory Defaults ” on page 325](#)
- [“Reset Factory Defaults for SP and Oracle ILOM BIOS” on page 326](#)
- [“Back Up the BIOS Configuration ” on page 327](#)
- [“Restore BIOS Configuration ” on page 328](#)

▼ Reset BIOS Configuration to Factory Defaults

Before You Begin

- Review the [“Requirements for BIOS Configuration Tasks” on page 323](#).
- **Perform one of the following actions to reset the BIOS non-volatile data store parameters to factory defaults:**
 - From the web interface, click System Management > BIOS, then select Factory from the Reset To Defaults list box and click Save.
 - From the CLI, type: `set /System/BIOS reset_to_defaults=factory`

Oracle ILOM resets the BIOS Setup parameters in the non-volatile data store to factory defaults. The Reset To Defaults value reverts to None after the factory default parameters are applied.

Related Information:

- [“View the BIOS Configuration Sync Status and Sync the Configuration Parameters” on page 324](#)
- [“Reset Factory Defaults for SP and Oracle ILOM BIOS” on page 326](#)
- [“Back Up the BIOS Configuration ” on page 327](#)
- [“Restore BIOS Configuration ” on page 328](#)

▼ Reset Factory Defaults for SP and Oracle ILOM BIOS

Before You Begin

- Review the [“Requirements for BIOS Configuration Tasks” on page 323](#)

Follow these steps to reset the Oracle ILOM configuration and the host BIOS configuration to factory defaults from the Oracle ILOM CLI or web interface.

1. Power off the host operating system on the managed Oracle x86 server by performing one of the following:

- From the web interface, click Host Management > Power Control > Power Cycle.
- From the CLI, type: **stop -force /System**

2. Reset the parameters in BIOS non-volatile data store to factory defaults by performing one of the following:

- From the web interface, click System Management > BIOS, then select Factory from the Reset Defaults To Factory list box, and click Save.
- From the CLI, type: **set /System/BIOS reset_to_defaults=factory**

Note - Wait until `/System/BIOS reset_to_defaults` changes from *factory* to *none* before proceeding with Step 3. The `reset_to_defaults` value reverts back to *none* after the factory defaults have been applied to the host BIOS non-volatile data store.

3. Reset the Oracle ILOM configuration to factory defaults by performing one of the following:

- From the web interface, click ILOM Administration> Configuration Management > Reset Defaults, then select Factory from the Reset Defaults list box, and click Reset Defaults.
- From the CLI, type: **set /SP reset_to_defaults=factory**

4. Power cycle the Oracle ILOM SP by performing one of the following:

- From the web interface, click Host Management > Power Control > Reset.
- From the CLI, type: `reset /SP`

Oracle ILOM resets BIOS configuration parameters to factory defaults and returns None as the Sync Status state.

Related Information:

- [“View the BIOS Configuration Sync Status and Sync the Configuration Parameters” on page 324](#)
- [“Reset BIOS Configuration to Factory Defaults ” on page 325](#)
- [“Back Up the BIOS Configuration ” on page 327](#)
- [“Restore BIOS Configuration ” on page 328](#)

▼ Back Up the BIOS Configuration

Before You Begin

- Review the [“Requirements for BIOS Configuration Tasks” on page 323](#).
- The Backup BIOS Configuration operation typically takes two to three minutes to complete.

Follow this procedure to back up the parameters from BIOS non-volatile data store to the Oracle ILOM BIOS Configuration file.

1. To back up the BIOS configuration, perform one of the following:

- From the web interface, click System Management > BIOS, in the Backup section select an option from the Transfer Method list box, then specify the required parameters for the Transfer Method, and click Start Backup.

- From the CLI, type:

```
set dump_uri transfer_method://username:password@ipaddress_or_hostname/
directorypath/filename
```

Where:

- *transfer_method* appears, type either: tftp, ftp, sftp, scp, http, or https
- *username* appears, type the name of the user account for the chosen transfer method server. A username is required for scp, sftp, and ftp. A username is not required for tftp, and it is optional for http and https.

- *password* appears, type the user account password for the chosen transfer method server. A password is required for scp, sftp, and ftp. A password is not used for tftp, and it is optional for http and https.
- *ipaddress_or_hostname* appears, type the IP address or the host name for the chosen transfer method server.
- *directorypath* appears, type the file storage location on the transfer method server.
- *filename* appears, type the name assigned to the Backup Configuration file, for example: `foo.xml`.

2. Wait while Oracle ILOM completes the BIOS Backup operation.

Oracle ILOM retrieves a copy of the BIOS non-volatile data store configuration file and saves it to the Oracle ILOM file system.

Related Information:

- [“Web and CLI: BIOS Properties” on page 319](#)
- [Table 92, “-force Option for CLI Commands: load and dump,” on page 322](#)
- [“View the BIOS Configuration Sync Status and Sync the Configuration Parameters” on page 324](#)
- [“Reset BIOS Configuration to Factory Defaults ” on page 325](#)
- [“Reset Factory Defaults for SP and Oracle ILOM BIOS” on page 326](#)
- [“Restore BIOS Configuration ” on page 328](#)

▼ Restore BIOS Configuration

Before You Begin

- Review the [“Requirements for BIOS Configuration Tasks” on page 323](#).
- The data in the boot device section of the Oracle ILOM Configuration file is read-only and does not affect the parameters restored to the BIOS non-volatile data store.
- The BIOS Configuration Restore operation typically takes two to three minutes to complete.

Follow this procedure to restore the parameters in the Oracle ILOM BIOS Configuration file to the BIOS non-volatile data store.

1. To restore the BIOS configuration, perform one of the following:

- From the web interface, click System Management > BIOS, select a Restore Option, select a Transfer Method option, then specify the required parameters for the Transfer Method, and click Start Restore.

- From the CLI, type:

```
set load_uri=restore_option/transfer_method://username:password@ipaddress_  
or_hostname/directorypath/filename
```

Where:

- *restore_option* appears, type either: all, config-only, or bootlist-only
- *transfer_method* appears, type either: tftp, ftp, sftp, scp, http, or https
- *username* appears, type the user account name for the chosen transfer method server. A user name is required for scp, sftp, and ftp. A user name is not required for tftp, and it is optional for http and https.
- *password* appears, type the user account password for the chosen transfer method server. A password is required for scp, sftp, and ftp. A password is not used for tftp, and it is optional for http and https.
- *ipaddress_or_hostname* appears, type the IP address or the host name for the chosen transfer method server.
- *directorypath* appears, type the storage location for the Oracle ILOM Configuration file (/System/BIOS/Config) on the transfer method server.
- *filename* appears, type the name assigned to the Oracle ILOM Configuration file, for example: foo.xml.

Note - To cancel a pending restore BIOS configuration action, type: `set action=cancel`

2. Wait while Oracle ILOM completes the Restore operation.

Oracle ILOM exports the BIOS configuration parameters from the Oracle ILOM BIOS Configuration file to the BIOS non-volatile data store, and updates the state of the Restore Status.

3. Verify the state of the Restore Status to determine whether the Restore operation succeeded.

For a list of Restore Status state descriptions, see the [“Web and CLI: BIOS Properties” on page 319](#).

Note - Restore operation results are logged in the Oracle ILOM event log (/SP/logs/event list).

Related Information

- [“Web and CLI: BIOS Properties” on page 319](#)

- [Table 92, “-force Option for CLI Commands: load and dump,” on page 322](#) **-force**
Option for CLI Commands: load and dump
- [“View the BIOS Configuration Sync Status and Sync the Configuration Parameters” on page 324](#)
- [“Reset BIOS Configuration to Factory Defaults ” on page 325](#)
- [“Reset Factory Defaults for SP and Oracle ILOM BIOS” on page 326](#)
- [“Back Up the BIOS Configuration ” on page 327](#)

SAS Zoning Chassis Blade Storage Resources

Description	Links
Refer to this section to learn about supported management options for zoning chassis-level storage devices.	■ “Zone Management for Chassis-Level SAS-2 Capable Resources” on page 331
Refer to this section for information about Oracle ILOM Sun Blade Zone Manager properties.	■ “Sun Blade Zone Manager Properties ” on page 333
Refer to this section for important information about saving, backing up, and recovering SAS zoning configuration parameters.	■ “Important SAS Zoning Allocations Considerations ” on page 341
Refer to this section for procedures for enabling the Sun Blade Zone Manager and creating SAS zoning assignments.	■ “Enabling Zoning and Creating SAS-2 Zoning Assignments” on page 342
Refer to this section for procedures for viewing or modifying existing storage allocations.	■ “Managing Existing SAS-2 Storage Resource Allocations” on page 358
Refer to this section for resetting all saved storage allocations to factory defaults.	■ “Resetting Sun Blade Zone Manager Allocations to Factory Defaults” on page 367
Refer to this section to optionally reset the in-band management password.	■ “Resetting the Zoning Password to Factory Default for Third-Party In-Band Management ” on page 368

Zone Management for Chassis-Level SAS-2 Capable Resources

Oracle ILOM provides zone management support for chassis-level SAS-2 storage devices installed in an Oracle blade chassis system. You can choose to manage access to the blade chassis-level storage resources by using the Oracle ILOM Sun Blade Zone Manager or a third-party in-band application. For more details, see:

- [“Zone Management Using a Third-Party In-Band Management Application” on page 332](#)
- [“Zone Management Using Oracle ILOM Sun Blade Zone Manager” on page 332](#)
- [“Manageable SAS-2 Zoning-Capable Devices” on page 332](#)

Zone Management Using a Third-Party In-Band Management Application

If your environment supports managing access to chassis-level storage devices using a third-party in-band management application, you should verify that the state for the Sun Blade Zone Manager in Oracle ILOM is disabled (default). If you need to reset the in-band management password to factory defaults, you can reset this password in Oracle ILOM. For instructions, see [“Resetting the Zoning Password to Factory Default for Third-Party In-Band Management” on page 368](#).

Zone Management Using Oracle ILOM Sun Blade Zone Manager

When the Sun Blade Zone Manager is enabled in the Oracle ILOM CMM you can manage chassis-level SAS-2 storage permissions to Oracle blade CPU servers installed in the chassis. For further details about using the Oracle ILOM Sun Blade Zone Manager, see these topics:

- [“Manageable SAS-2 Zoning-Capable Devices” on page 332](#)
- [“Sun Blade Zone Manager Properties” on page 333](#)
- [“Important SAS Zoning Allocations Considerations” on page 341](#)
- [“Enabling Zoning and Creating SAS-2 Zoning Assignments” on page 342](#)
- [“Managing Existing SAS-2 Storage Resource Allocations” on page 358](#)
- [“Resetting Sun Blade Zone Manager Allocations to Factory Defaults” on page 367](#)

Manageable SAS-2 Zoning-Capable Devices

The Oracle ILOM CMM recognizes the following devices in an Oracle blade chassis system as manageable SAS-2 zoning-capable devices:

- Oracle blade CPU server with SAS-2 RAID expansion modules (REMs)
- Oracle blade chassis system Network express modules (NEMs)
- Oracle blade storage server (such as Oracle's Sun Blade Storage Module M2)

Note - Oracle ILOM does not support zoning management for: (1) internal storage modules installed on an Oracle blade CPU server; (2) Fabric Expansion Modules (FMODs) on an Oracle storage blade; or, (3) external network SAS-2 storage resources that are connected to an Oracle blade chassis system through the external SAS-2 ports of a NEM.

Note - The Sun Blade Zone Manager CLI will not recognize or list the presence of non-manageable, non-supporting SAS-2 storage devices. However, in some instances, the Sun Blade Zone Manager web interface might recognize and list the presence of non-manageable, non-supporting SAS-2 storage devices. In these cases, the non-SAS-2 storage devices in the Sun Blade Zone Manager web interface are labeled as non-SAS-2 resources.

Sun Blade Zone Manager Properties

Oracle ILOM provides a set of easy-to-use properties for setting up and managing access permissions to chassis-level SAS-2 storage devices. For more details, see:

- [“Sun Blade Zone Manager Web: Properties” on page 333](#)
- [“Sun Blade Zone Manager CLI: Targets and Properties” on page 340](#)

Sun Blade Zone Manager Web: Properties

The Sun Blade Zone Manager Settings page is accessible from the Oracle ILOM CMM web interface by clicking System Management > SAS Zoning. The Sun Blade Zone Manager Settings page provides the following options for enabling, setting up, and managing SAS zoning permissions:

- [“Sun Blade Zone Manager: State” on page 333](#)
- [“Whole Chassis Setup: Quick Setup” on page 334](#)
- [“Full Resource Control: Detailed Setup” on page 338](#)
- [“Zoning Reset: Reset All ” on page 339](#)

Sun Blade Zone Manager: State

The state for the Sun Blade Zone Manager in the Oracle ILOM CMM web interface appears on the Sun Blade Zone Manager Settings page.

When this state is enabled, the Sun Blade Zone Manager provides template-based (Quick Setup) or custom zoning capabilities (Detailed Setup) for chassis-installed SAS-2 storage devices.

When this state is disabled (default), Oracle ILOM is unable to manage the access permissions to the chassis-installed SAS-2 storage devices, and the options for Quick Setup and Detailed Setup are hidden from view on the Sun Blade Zone Manager Settings page.

For instructions for enabling the Sun Blade Zone Manager state, see [“Access and Enable Sun Blade Zone Manager ” on page 343](#).

Whole Chassis Setup: Quick Setup

The Whole Chassis Setup feature, in the web interface, is typically used when setting up zoning access for the first time for all chassis-level SAS-2 storage devices. This feature offers the following Quick Setup zoning options:

- [“Option 1: Assign to Individual Disks \(Quick Setup\)” on page 334](#)
- [“Option 2: Assign to Adjacent Individual Disks \(Quick Setup\)” on page 335](#)
- [“Option 3: Assign to Individual Storage Blade \(Quick Setup\)” on page 336](#)
- [“Option 4: Assign to Adjacent Storage Blade \(Quick Setup\) ” on page 337](#)

Option 1: Assign to Individual Disks (Quick Setup)

The first zoning option, shown in the Quick Setup dialog, uses a round-robin algorithm to evenly allocate storage ownership across all chassis CPU blade servers.

Option 1 is best suited for fault-tolerant chassis system operation where the failure or removal of a single storage blade server will not bring down all storage arrays.

Note - Empty slots shown in the Quick Setup dialog represent chassis blade slots that are empty (nothing installed).

The second zoning allocation option, shown in the Quick Setup dialog, equally divides the number of blade storage disks among the adjacent CPU blade servers.

Option 2 attempts to allocate the same number of storage disks as possible to each adjacent CPU blade server. If there are no storage blades adjacent to a CPU blade, then Sun Blade Zone Manager will allocate storage disks from the nearest possible storage blade.

The third zoning allocation option, shown in the Quick Setup dialog, scans the blade chassis system for CPU blade servers (starting at Slot 0) and then assigns the storage disks from the closest available storage blade.

336

Note - NEM0 and NEM1 targets appear in the Zone Manager when these NEMs are installed; however, external NEM connections to SAS-2 network storage devices are not supported or shown in the Sun Blade Zone Manager.

Full Resource Control: Detailed Setup

- Add storage allocations to a CPU blade server by clicking components outside the color-coded server group.
- Remove storage resource allocations assigned to a CPU blade server by clicking components within a color-coded server group
- Share a single resource allocation between one or more CPU blade servers.

- “Allocate Storage Resources to Single Blade Server: Detailed Setup (Web)” on page 347
- “Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup (Web)” on page 352
- “Modify Existing Blade Group Allocations (Web)” on page 361

For instructions for resetting the Sun Blade Zone Manager parameters to factory defaults, see [“Reset Zoning Allocations to Factory Defaults \(Web\)”](#) on page 367.

Sun Blade Zone Manager CLI: Targets and Properties

The Oracle ILOM CMM CLI provides access to zoning targets and properties under the `/STORAGE/sas_zoning` namespace.

SAS Zoning Properties	Values	Default	Description
zone_management_state=	<i>disabled</i> <i>enabled</i>	Disabled	When set to disabled, the Sun Blade Zone Manager is unable to manage the SAS-2 chassis storage resources. When set to enabled, the Sun Blade Zone Manager provides template-based or custom zoning capabilities for chassis-installed SAS-2 resources.
reset_password_action=	<i>true</i>		When set to true, the in-band management zoning password on the CMM is set to factory defaults (all zeros).
reset_access_action=	<i>true</i>		When set to true, the storage resource allocation parameters currently saved on the CMM are set to factory defaults.

When zoning is enabled, blades and NEMs that are SAS-2 capable appear as CLI targets under `/STORAGE/sas_zoning`. For example:

```
-> show /STORAGE/sas_zoning

Targets
  BL0
  BL6
  BL7
  BL8
  BL9
  NEM0
  NEM1

Properties
  zone_management_state = enabled
  reset_password_action = (Cannot show property)
  reset_access_action = (Cannot show property)

Commands:
  cd
  set
  show
```

Note - NEM0 and NEM1 targets appear in the Zone Manager when these NEMs are installed; however, external SAS connections in the Sun Blade Zone Manager are not supported at this time.

SAS-2 capable storage devices on a blade server appear as targets under `sas_zoning/BLn`. For example:

```
-> show /STORAGE/sas_zoning/BL9
```

Targets:

```
HDD0
HDD2
HDD3
HDD5
```

The SAS zoning properties that are available under the blade target (`BLn`) or storage device (`HDDn`) target include:

Blade and Storage Properties	SAS Zoning Target	Description
<code>add_storage_access=</code>	<code>/BLn</code>	Use the <code>add_storage_access=</code> property under the <code>/sas_zoning/BLn</code> target to allocate storage to a CPU blade server.
<code>remove_storage_access=</code>	<code>/BLn</code>	Use the <code>remove_storage_access=</code> property under the <code>/sas_zoning/BLn</code> target to remove storage from a CPU blade server.
<code>add_host_access=</code>	<code>/BLn/HDDn</code>	Use the <code>add_host_access=</code> property under the <code>/sas_zoning/BLn/HDDn</code> target to allocate storage to a CPU blade server.
<code>remove_host_access=</code>	<code>/BLn/HDDn</code>	Use the <code>remove_host_access=</code> property under the <code>/sas_zoning/BLn/HDDn</code> target to remove storage from a CPU blade server.

For further instructions on how to manage storage resource allocations from the Oracle ILOM CLI, see:

- [“Manually Create SAS-2 Zoning Allocations \(CLI\)” on page 356](#)
- [“View and Modify Existing Storage Allocations \(CLI\)” on page 365](#)
- [“Reset Zoning Allocations to Factory Defaults \(CLI\)” on page 368](#)
- [“Reset the Zoning Password \(CLI\)” on page 369](#)

Important SAS Zoning Allocations Considerations

- [“Saving Storage Allocations” on page 342](#)

- [“Backing Up and Recovering SAS-2 Zoning Assignments” on page 342](#)

Saving Storage Allocations

When you save storage allocations to a blade, consider the following:

- The storage allocations saved in Oracle ILOM are based on the hardware currently installed in the chassis (SAS-2 NEMs or storage blades). Changes in the chassis hardware configuration can result in a loss of a storage blade group. Therefore, you should back up all chassis storage allocations in Oracle ILOM. For more information, see [“Backing Up and Recovering SAS-2 Zoning Assignments” on page 342](#).

Note - Hot-plugging of chassis components such as NEMs and storage blades can also affect the storage blade group allocations. For further information on the effects of hot-plugging NEMs and storage blades, refer to the Oracle storage blade or NEM hardware documentation.

- The Sun Blade Zone Manager dialog (Modify Group or New Assignments) must remain open during the entire Save operation. If the Sun Blade Zone Manager dialog is closed while the Save operation is in progress, only a portion of the storage blade group will be preserved.
- Do not remove or power cycle any of the chassis hardware components that are part of a storage blade group while a Save operation is in progress. Doing so will cause the group allocation not to save properly.

Backing Up and Recovering SAS-2 Zoning Assignments

Oracle ILOM provides Backup and Restore operations that enable you to: (1) create a backup copy of all parameters saved in the Oracle ILOM Configuration file, and (2) restore a backup copy of the Oracle ILOM Configuration file. For details about how to create a backup copy or how to restore a backup copy of the Oracle ILOM Configuration file, see [“SAS Zoning Chassis Blade Storage Resources ” on page 331](#).

Enabling Zoning and Creating SAS-2 Zoning Assignments

- [“Chassis Hardware Requirements” on page 343](#)

- [“Access and Enable Sun Blade Zone Manager ” on page 343](#)
- [“Allocating Storage to Entire Chassis: Quick Setup \(Web\)” on page 345](#)
- [“Allocate Storage Resources to Single Blade Server: Detailed Setup \(Web\)” on page 347](#)
- [“Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup \(Web\)” on page 352](#)
- [“Manually Create SAS-2 Zoning Allocations \(CLI\)” on page 356](#)

Chassis Hardware Requirements

- A PCIe 2.0 compliant midplane must exist in the Sun Blade 6000 chassis. For more information on determining this, refer to the *Sun Blade 6000 Modular System Product Notes*.
- The minimum software release of 3.2.1 must be installed on the CMM. This release includes the minimum Oracle ILOM CMM firmware version (3.0.10.15a), which supports SAS-2 and includes the Sun Blade Zone Manager.
- All SAS-2 storage devices (blade server module with SAS-2 REM, SAS-2 NEMs, and SAS-2 storage modules) must be properly installed and powered-on in the Oracle blade chassis system.

Note - If the state of a SAS-2 storage device is in a failed state, the Sun Blade Zone Manager might not be able to recognize the failed SAS-2 storage device.

- SAS-2 NEMs must be at a firmware version level that supports zoning. Check your NEM product notes for version information and available updates.
- Initial setup and configuration of your Oracle ILOM CMM must be completed. For information about establishing a management connection to the Oracle ILOM CMM, see [“Setting Up a Management Connection to Oracle ILOM and Logging In” on page 17](#).

▼ Access and Enable Sun Blade Zone Manager

Before You Begin When enabled, the Sun Blade Zone Manager in Oracle ILOM provides a way of constraining which CPU blade servers within a SAS domain have access to storage resources (HDDs, FMODs, external SAS ports).

Before You Begin

- The Admin (a) role is required in Oracle ILOM to modify SAS Zoning properties.
- Review [“Chassis Hardware Requirements” on page 343](#).

- Review [“Important SAS Zoning Allocations Considerations ” on page 341.](#)

Note - The presence of chassis storage blades in the Oracle ILOM web interface are not shown in the CMM Manage menu. Storage disks installed on storage blade servers are viewable from the System Information > Storage page. Oracle storage blade resource allocations are manageable from the System Management > SAS Zoning > Sun Blade Zone Manager Settings page.

1. To access and enable the Sun Blade Zone Manager from the CMM web interface, perform these steps:

a. Click System Management > SAS Zoning.

The Sun Blade Zone Manager Settings page appears.

b. Enable SAS Zoning by selecting the Enabled check box and clicking Save.

After enabling the Sun Blade Zone Manager, you can create, view, and manage settings for SAS-2 zoning using Oracle ILOM interfaces.

The following message might appear if the Oracle ILOM CMM services are still initializing:

```
Sun Blade Zone Manager Not Ready
The Sun Blade Zone Manager is initializing and not ready for .
operation. Please wait several minutes and then refresh to check
the status
```

If the above message appears, wait five minutes and then try again. You will need to close and reopen, or refresh the web interface page.

2. To enable the SAS Zoning property from the CMM CLI, type:

```
set /STORAGE/SAS_zoning zone_management_state=enabled
```

■ **The following message appears.**

Enabling the Sun Blade Zone Manager will result in the clearing of all zoning configuration in the installed chassis SAS hardware, and any SAS disk I/O in progress will be interrupted.

Are you sure you want to enable the Sun Blade Zone Manager (y/n)?

■ **To continue, type: y**

The following message appears.

Set 'zone_management_state' to 'enabled'

- **If the Oracle ILOM CMM is unable to initialize the Sun Blade Zone Manager, the following message appears:**

set: The Sun Blade Zone Manager is initializing and not ready for operation. Please wait several minutes and try again.

If the above message appears, wait five minutes and retry the command.

Related Information

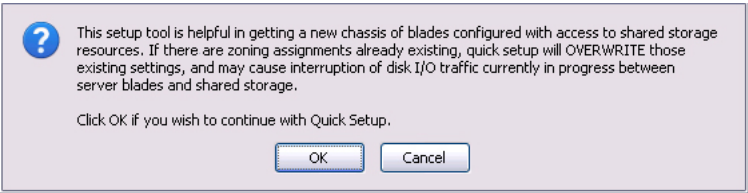
- [“Allocating Storage to Entire Chassis: Quick Setup \(Web\)” on page 345](#)
- [“Allocate Storage Resources to Single Blade Server: Detailed Setup \(Web\)” on page 347](#)
- [“Manually Create SAS-2 Zoning Allocations \(CLI\)” on page 356](#)
- [“Managing Existing SAS-2 Storage Resource Allocations” on page 358](#)
- [“Resetting Sun Blade Zone Manager Allocations to Factory Defaults” on page 367](#)

▼ Allocating Storage to Entire Chassis: Quick Setup (Web)

Before You Begin:

- The Admin (a) role is required in Oracle ILOM to modify SAS Zoning properties.
 - Review [“Chassis Hardware Requirements” on page 343](#).
 - SAS Zoning must be enabled in Oracle ILOM prior to performing this Quick Setup procedure for assigning zoning. For instructions, see [“Access and Enable Sun Blade Zone Manager ” on page 343](#).
1. **To access the Sun Blade Zone Manager Settings page in the web interface, click System Management > SAS Zoning.**
 2. **In the Sun Blade Zone Manager section, click the Quick Setup button.**

A warning message appears.



3. To overwrite existing zoning assignments, click OK.

The Quick Setup screen appears.

Quick Setup

Select how you would like all chassis storage resources allocated and click 'Save'.

☐ 1. Assign per individual disks.

☐ 2. Assign per adjacent individual disks.

☐ 3. Assign per storage blade.

☐ 4. Assign per adjacent storage blade.

Save

SUN BLADE 6000 MODULAR SYSTEM - bur_02_core_1lom

Slot 0 Server Blade Sun Blade X8670 M2	Slot 1 Server Blade Sun Blade X8670 M2	Slot 2 Storage Blade Sun Blade Storage Module M2	Slot 3 Server Blade Sun Blade X8670 M2	Slot 4 Server Blade Sun Blade X8670 M2	Slot 5 Storage Blade Sun Blade Storage Module M2	Slot 6 Storage Blade Sun Blade Storage Module M2	Slot 7 Server Blade Sun Blade X8670 M2	Slot 8 Storage Blade Sun Blade Storage Module M2	Slot 9 Storage Blade Sun Blade Storage Module M2
		HDD 6HDD 7 HDD 4HDD 5 HDD 2HDD 3 HDD 0HDD 1			HDD 6HDD 7 HDD 4HDD 5 HDD 2HDD 3 HDD 0HDD 1	HDD 6HDD 7 HDD 4HDD 5 HDD 2HDD 3 HDD 0HDD 1		HDD 6HDD 7 HDD 4HDD 5 HDD 2HDD 3 HDD 0HDD 1	HDD 6HDD 7 HDD 4HDD 5 HDD 2HDD 3 HDD 0HDD 1
		emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty			emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty	emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty		emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty	emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty emptyempty

NEM Slot 0

SAS NEM

NEM-2

EXT 0EXT 1EXT 2EXT 3

NEM Slot 1

SAS NEM

NEM-2

EXT 0EXT 1EXT 2EXT 3

NAC name:

/CH/BL6/FMOD22

Disk type:

SAS

WWN:

80205010.33333336 80205010.33333337

Note - Any HDD chassis slot that does not have a HDD presently installed in the chassis is labeled “empty.” Empty HDD chassis slots are not included in the Quick Setup storage assignments.

4. **To indicate how you would like to allocate the chassis storage resources, select one of the Quick Setup options.**

For a description of each Quick Setup option, see [“Whole Chassis Setup: Quick Setup” on page 334](#).

After choosing a Quick Setup option, the Sun Blade Zone Manager displays the color-coded zoning allocations between the CPU blade servers and storage devices (HDDs) installed on the storage blade servers. Although the Sun Blade Zone Manager shows the NEM0 and NEM1 External SAS connections, these connections are not supported.

Note - Until you click the Save button, the chassis storage allocations are not saved.

5. **To save the Quick Setup chassis storage allocations, click Save.**
6. **To back up the newly saved blade storage group allocations, see [“Backing Up and Recovering SAS-2 Zoning Assignments” on page 342](#).**

Related Information

- [“Important SAS Zoning Allocations Considerations ” on page 341](#)
- [“Allocate Storage Resources to Single Blade Server: Detailed Setup \(Web\)” on page 347](#)
- [“Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup \(Web\)” on page 352](#)
- [“Modify Existing Blade Group Allocations \(Web\)” on page 361](#)
- [“Manually Create SAS-2 Zoning Allocations \(CLI\)” on page 356](#)
- *Sun Blade 6000 Modular System Documentation*

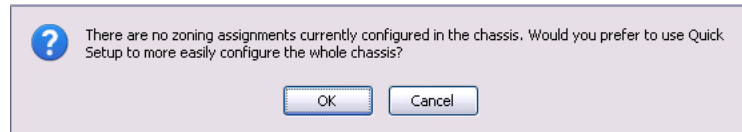
▼ Allocate Storage Resources to Single Blade Server: Detailed Setup (Web)

Before You Begin:

- The Admin (a) role is required in Oracle ILOM to modify SAS Zoning properties.
- Review [“Chassis Hardware Requirements” on page 343](#).

- The Sun Blade Zone Manager must be enabled in Oracle ILOM prior to performing this procedure. For instructions, see [“Access and Enable Sun Blade Zone Manager” on page 343](#).
1. **In the Sun Blade Zone Manager Settings page, click the Detailed Setup button.**
One of the following appears:

- **The Zoning Config dialog appears. Proceed to Step 3.**
- **The following message appears indicating no zoning assignments exist. Proceed to Step 2.**



2. **In the message that states no zoning assignments exist, perform one of the following:**
 - **If you want to manually create SAS zoning assignments using the Detailed Setup option, click Cancel and proceed to Step 4.**

Clicking Cancel will open the Detailed Setup Zoning Config page.

Zoning Config
 The current access permission assignments are displayed below. Click 'New Assignments' to make new access groupings. Or, click on any component to select all those to which it has access assigned, then click 'Modify Group' to make changes to that selected group.

SUN BLADE 6000 MODULAR SYSTEM - bur_02_core_0lom

Slot 0 Server Blade	Slot 1 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 empty	Slot 2 Server Blade	Slot 3 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 empty	Slot 4 Server Blade	Slot 5 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 empty	Slot 6 Server Blade	Slot 7 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 empty	Slot 8 Server Blade	Slot 9 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 empty
-------------------------------	--	-------------------------------	--	-------------------------------	--	-------------------------------	--	-------------------------------	--

NEM Slot 0
 SAS NEM
 NEM-2
 EXT 0 EXT 1 EXT 2 EXT 3

NEM Slot 1
 SAS NEM
 NEM-2
 EXT 0 EXT 1 EXT 2 EXT 3

NAC name: -

Disk type: -

WWN: -

- If you want to set up the initial zoning assignments using Sun Blade Zone Manager Quick Setup option, click OK and proceed to [“Allocating Storage to Entire Chassis: Quick Setup \(Web\)” on page 345](#).
- 3. To assign storage resources to a single blade server, perform these steps in the Zoning Config dialog:
 - a. Click **New Assignments**.
 New Assignments dialog appears.

- b. Click a blade server then click the storage resources (HDDs) that you want to assign to the selected blade server.

Note - All HDD chassis slots that do not have an HDD storage device installed are labeled “empty.” Empty HDD chassis slots are not allocated to CPU blade servers.



Caution - Alternatively, you can allocate storage resources to multiple blade servers; however, the servers must be enabled for multipathing. For further instructions, see [“Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup \(Web\)”](#) on page 352.

Although the Sun Blade Zone Manager displays them, NEM0 and NEM1 External SAS connections are not supported.

New Assignment

Click on components to include in a new access group and click 'Save'.

Save

Cancel

SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-0000000-0000000000

Slot 0 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 1 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 (select all) empty	Slot 2 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 3 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 (select all) empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	Slot 4 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 5 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 (select all) empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	Slot 6 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 7 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 (select all) empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	Slot 8 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 9 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 (select all) empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty
---	---	---	--	---	--	---	--	---	--

NEM Slot 0

SAS NEM NEM-2

EXT 0 EXT 1 EXT 2 EXT 3

NEM Slot 1

SAS NEM NEM-2

EXT 0 EXT 1 EXT 2 EXT 3

NAC name:

Disk type:

WWN:

▼ Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup (Web)

Before You Begin



Caution - Refer to the Oracle blade server documentation to determine whether the server is enabled for sharing storage resources with another Oracle blade server.



Caution - The option for sharing a single storage resource should only be used with an Oracle-supported clustering solution. For more information about clustering solutions, see the *Sun Blade Storage Module Administration Guide*.

- The Admin (a) role is required in Oracle ILOM to modify SAS Zoning properties.
 - Review [“Chassis Hardware Requirements” on page 343](#).
 - The Sun Blade Zone Manager must be enabled in Oracle ILOM prior to performing this procedure. For instructions, see [“Access and Enable Sun Blade Zone Manager” on page 343](#).
1. In the **Sun Blade Zone Manager Settings** page, click the **Detailed Setup** button.

example, HDD6 in slot 2) that you want to share with this target (for example, in slot 1).

New Assignment

Click on components to include in a new access group and click 'Save'.

Save

Cancel

SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-0000000-0000000000

Slot 0 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 1 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 2 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 [select all] empty	Slot 3 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 4 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 5 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 [select all] empty	Slot 6 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 7 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 [select all] empty	Slot 8 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 9 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 [select all] empty
---	---	---	---	---	---	---	---	---	---

NEM Slot 0

SAS NEM NEM-2

EXT 0

EXT 1

EXT 2

EXT 3

NEM Slot 1

SAS NEM NEM-2

EXT 0

EXT 1

EXT 2

EXT 3

NAC name:

-

Disk type:

-

WWN:

-

- c. To save the allocation modification to the blade storage group, click Save. The following message appears.

This will apply the add and remove changes you have specified.

Be aware that the changes specified will result in the following storage components being accessible by more than one server blade.

/CH/BL1/HDD6

This configuration is only supported in certain environments (such as clustering). Check your system documentation to ensure that this configuration is supported to avoid possible data loss.

Do you wish to continue?

Cancel

OK

- The Sun Blade Zone Manager highlights the shared storage resources in pink.

The HDD6 storage resource in slot 2 is highlighted with pink to indicate this resource is shared by more than one CPU blade server.

- ## Related Information

- [“Managing Existing SAS-2 Storage Resource Allocations” on page 358](#)
- *Sun Blade 6000 Modular System Documentation*

▼ Manually Create SAS-2 Zoning Allocations (CLI)

Before You Begin

- Ensure that your chassis configuration meets the requirements in [“Chassis Hardware Requirements” on page 343](#).
- Admin (a) role privileges are required to manually create SAS zoning allocations in Oracle ILOM.
- The Sun Blade Zone Manager must be enabled in Oracle ILOM.

1. Access the Sun Blade Zone Manager from the CLI.

For instructions, see [“Access and Enable Sun Blade Zone Manager” on page 343](#).

2. Use one of the following methods to allocate a storage resource to a CPU blade server:

- **Method 1:** To assign a storage disk to a CPU blade server, use the following commands:

```
-> cd /STORAGE/sas_zoning/BLn
-> set add_storage_access=path_to_storage_disk
```

Where BLn is the chassis slot number for the CPU blade server and *path_to_storage_disk* is the path to the storage blade disk that you want to assign to the CPU blade server.

For example, to assign the hard disk drive in the storage blade slot location 0 to the CPU blade server in chassis slot location 1, you would type:

```
-> set add_storage_access=/CH/BL1/HDD0.
```

- **Method 2:** To assign CPU blade server to a storage resource, type:

```
-> cd /STORAGE/sas_zoning/BLn/HDDn
-> set add_host_access=path_to_blade_server
```

Where BLn is the chassis slot location for the CPU blade server, HDDn is storage blade slot location for the hard disk drive, and *path_to_blade_server* is the CPU blade server target where you want to assign to the storage disk.

For example, if you wanted to assign a hard disk drive within a storage blade server to a CPU blade server in the chassis, you would type:

```
-> cd /STORAGE/sas_zoning/BL1/HDD0
-> set add_host_access=/CH/BL0
```

The following examples show how to use these commands to set up zoning assignments between storage devices on a storage blade in slot 1 and a server blade in slot 0.

■ **Method 1** - Command examples for allocating storage resources to a CPU blade server:

CLI Command Syntax Examples	Instructions
-> cd /STORAGE/sas_zoning/BL0	1. Use the first command syntax example to access the CPU blade server that will be assigned a storage resource.
-> set add_storage_access=/CH/BL1/HDD0	2. Use the second command syntax example to allocate the storage module (HDD0) in the storage blade server (BL1) to the host CPU blade server (BL0) in chassis slot 0.
-> set add_storage_access=/CH/BL1/HDD0,/CH/BL1/HDD1	3. Optionally, you can use the third command syntax to assign multiple devices in a single command line. Ensure that you specify the full path to the storage resource and separate each resource with a comma (no space).
-> show	4. Use the show command to confirm that the storage allocations are saved to the CPU blade server (/CH/BL1/HDD0 and CH/BL1/HDD1).
/STORAGE/sas_zoning/BL0	
Targets:	
0 (/CH/BL1/HDD0)	
1 (/CH/BL1/HDD1)	

■ **Method 2** - Command examples for assigning a CPU server blade (BL0) to a storage blade resource (BL1/HDD0):

CLI Command Syntax Examples	Instructions
-> cd /STORAGE/sas_zoning/BL1/HDD0	1. Use the first command syntax example to access the storage resource (HDD0) installed in the storage blade server (BL1/HDD0).
-> set add_host_access=/CH/BL0	2. Use the second command syntax example to assign the storage resource (HDD0) to the host CPU blade server (BL0).
-> show	3. Use the show command to confirm that the storage allocations are saved to the correct CPU blade server (/CH/BL0).
/STORAGE/sas_zoning/BL1/HDD0	
Targets:	
0 (/CH/BL0)	

3. Back up the newly saved server storage group.

Related Information

- [“Backing Up and Recovering SAS-2 Zoning Assignments” on page 342](#)
- [“Manually Create SAS-2 Zoning Allocations \(CLI\)” on page 356](#)
- *Sun Blade 6000 Modular System Documentation*

Managing Existing SAS-2 Storage Resource Allocations

The Sun Blade Zone Manager in Oracle ILOM enables you to manage existing allocations to chassis storage resources in the following ways:

- [“View Existing CPU Blade Server Storage Allocations \(Web\)”](#) on page 358
- [“Modify Existing Blade Group Allocations \(Web\)”](#) on page 361
- [“View and Modify Existing Storage Allocations \(CLI\)”](#) on page 365

▼ View Existing CPU Blade Server Storage Allocations (Web)

Before You Begin

- Admin (a) role privileges are required to view Sun Blade Zone Manager allocations in Oracle ILOM.
- The Sun Blade Zone Manager in Oracle ILOM must be enabled.

1. Access the Sun Blade Zone Manager and click Detailed Setup.

For instructions for accessing the Sun Blade Zone Manager, see [“Access and Enable Sun Blade Zone Manager ”](#) on page 343.

The Zoning Config dialog appears displaying the current chassis storage allocations.

Zoning Config

The current access permission assignments are displayed below. Click 'New Assignments' to make new access groupings. Or, click on any component to select all those to which it has access assigned, then click 'Modify Group' to make changes to that selected group.

New Assignments

Modify Group

SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-0000000-0000000000

Slot 0 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 1 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 2 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 empty	Slot 3 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 4 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 5 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 empty	Slot 6 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 7 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 empty	Slot 8 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 9 Storage Blade SUN BLADE STORAGE MODULE M2 HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1 empty
---	---	---	---	---	---	---	---	---	---

NEM Slot 0

SAS NEM

NEM-2

EXT 0

EXT 1

EXT 2

EXT 3

NEM Slot 1

SAS NEM

NEM-2

EXT 0

EXT 1

EXT 2

EXT 3

NAC name:

-

Disk type:

-

WWN:

-

2. To view all of the resource allocations for a selected CPU blade server, perform these steps:
- a. Select a CPU blade server slot.

For this example, slot 0 is selected.
- b. Scroll down to the Current Assignments table.

All of the storage resources that are currently assigned to the selected CPU blade server appear in the Current Assignments table.

Current Assignments for /CH/BL0		
Detach Table		
Component	Type	WWN
/CH/BL0	Server Blade (Virgo+)	-
/CH/NEM0/EXT0	SAS Port	-
/CH/NEM1/EXT0	SAS Port	-
/CH/BL2/HDD6	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD4	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD5	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD7	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/FMOD23	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD21	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD19	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD18	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD20	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD22	SAS FMOD	80205010:33333336 80205010:33333337

- To view, at the same time, the Current Assignments table for the selected CPU blade server and the resource allocations for the other chassis CPU blade servers, click **Detach Table**.

The detached Current Assignments table appears in a separate dialog box.

[\[Close\]](#)

Current Assignments for /CH/BL0		
Component	Type	WWN
/CH/BL0	Server Blade (Virgo+)	-
/CH/NEM0/EXT0	SAS Port	-
/CH/NEM1/EXT0	SAS Port	-
/CH/BL2/HDD6	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD4	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD5	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD7	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/FMOD23	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD21	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD19	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD18	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD20	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD22	SAS FMOD	80205010:33333336 80205010:33333337

Related Information

- [“Modify Existing Blade Group Allocations \(Web\)” on page 361](#)
- [“Important SAS Zoning Allocations Considerations ” on page 341](#)
- [“Manually Create SAS-2 Zoning Allocations \(CLI\)” on page 356](#)
- *Sun Blade 6000 Modular System Documentation*

▼ Modify Existing Blade Group Allocations (Web)

Before You Begin Before You Begin

- Ensure that your chassis hardware configuration meets the requirements described in [“Chassis Hardware Requirements” on page 343](#).
- Admin (a) role privileges are required in Oracle ILOM to modify any Sun Blade Zone Manager properties.
- The Sun Blade Zone Manager must be enabled in Oracle ILOM.

1. **To access the Sun Blade Zone Manager, click System Management > SAS Zoning.**

The SAS Zoning page appears.

2. **In the Sun Blade Zone Manager section, click Detailed Setup.**

The Zoning Config dialog appears, displaying the existing storage allocations in color-coded groups.

Zoning Config

The current access permission assignments are displayed below. Click 'New Assignments' to make new access groupings. Or, click on any component to select all those to which it has access assigned, then click 'Modify Group' to make changes to that selected group.

New Assignments

Modify Group

SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-0000000-0000000000

Slot 0 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 1 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 2 Storage Blade SUN BLADE STORAGE MODULE M2 <table><tr><td>HDD 6</td><td>HDD 7</td></tr><tr><td>HDD 4</td><td>HDD 5</td></tr><tr><td>HDD 2</td><td>HDD 3</td></tr><tr><td>HDD 0</td><td>HDD 1</td></tr></table> <table><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr></table>	HDD 6	HDD 7	HDD 4	HDD 5	HDD 2	HDD 3	HDD 0	HDD 1	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	Slot 3 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 4 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 5 Storage Blade SUN BLADE STORAGE MODULE M2 <table><tr><td>HDD 6</td><td>HDD 7</td></tr><tr><td>HDD 4</td><td>HDD 5</td></tr><tr><td>HDD 2</td><td>HDD 3</td></tr><tr><td>HDD 0</td><td>HDD 1</td></tr></table> <table><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr></table>	HDD 6	HDD 7	HDD 4	HDD 5	HDD 2	HDD 3	HDD 0	HDD 1	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	Slot 6 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 7 Storage Blade SUN BLADE STORAGE MODULE M2 <table><tr><td>HDD 6</td><td>HDD 7</td></tr><tr><td>HDD 4</td><td>HDD 5</td></tr><tr><td>HDD 2</td><td>HDD 3</td></tr><tr><td>HDD 0</td><td>HDD 1</td></tr></table> <table><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr></table>	HDD 6	HDD 7	HDD 4	HDD 5	HDD 2	HDD 3	HDD 0	HDD 1	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	Slot 8 Server Blade SUN BLADE X6270 M2 SERVER MODULE	Slot 9 Storage Blade SUN BLADE STORAGE MODULE M2 <table><tr><td>HDD 6</td><td>HDD 7</td></tr><tr><td>HDD 4</td><td>HDD 5</td></tr><tr><td>HDD 2</td><td>HDD 3</td></tr><tr><td>HDD 0</td><td>HDD 1</td></tr></table> <table><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr><tr><td>empty</td><td>empty</td></tr></table>	HDD 6	HDD 7	HDD 4	HDD 5	HDD 2	HDD 3	HDD 0	HDD 1	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty	empty
HDD 6	HDD 7																																																																																																																																								
HDD 4	HDD 5																																																																																																																																								
HDD 2	HDD 3																																																																																																																																								
HDD 0	HDD 1																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
HDD 6	HDD 7																																																																																																																																								
HDD 4	HDD 5																																																																																																																																								
HDD 2	HDD 3																																																																																																																																								
HDD 0	HDD 1																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
HDD 6	HDD 7																																																																																																																																								
HDD 4	HDD 5																																																																																																																																								
HDD 2	HDD 3																																																																																																																																								
HDD 0	HDD 1																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
HDD 6	HDD 7																																																																																																																																								
HDD 4	HDD 5																																																																																																																																								
HDD 2	HDD 3																																																																																																																																								
HDD 0	HDD 1																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								
empty	empty																																																																																																																																								

NEM Slot 0

SAS NEM

NEM-2

EXT 0	EXT 1	EXT 2	EXT 3
-------	-------	-------	-------

NEM Slot 1

SAS NEM

NEM-2

EXT 0	EXT 1	EXT 2	EXT 3
-------	-------	-------	-------

NAC name:

-

Disk type:

-

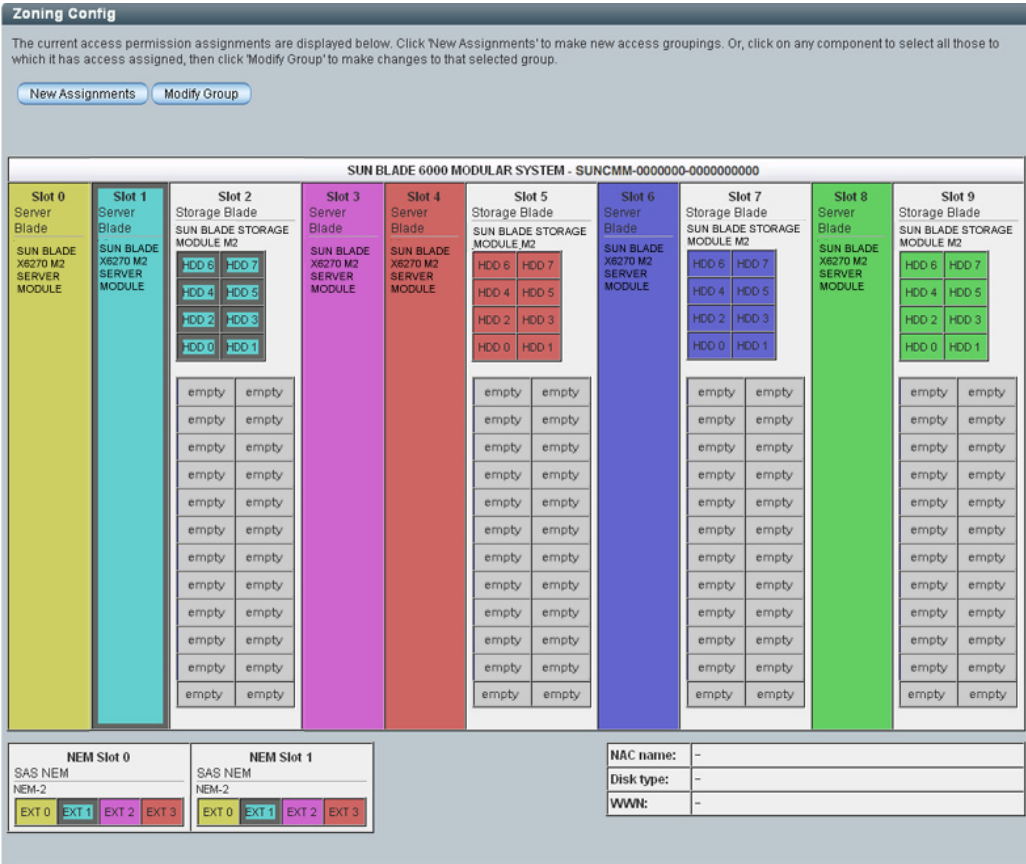
WWN:

-

Note - Any HDD slots that do not have a storage device installed are labeled “empty.” Empty HDD slots are not assigned to CPU blade servers.

3. To modify the storage allocations for a blade storage group, select a blade that is part of the group.

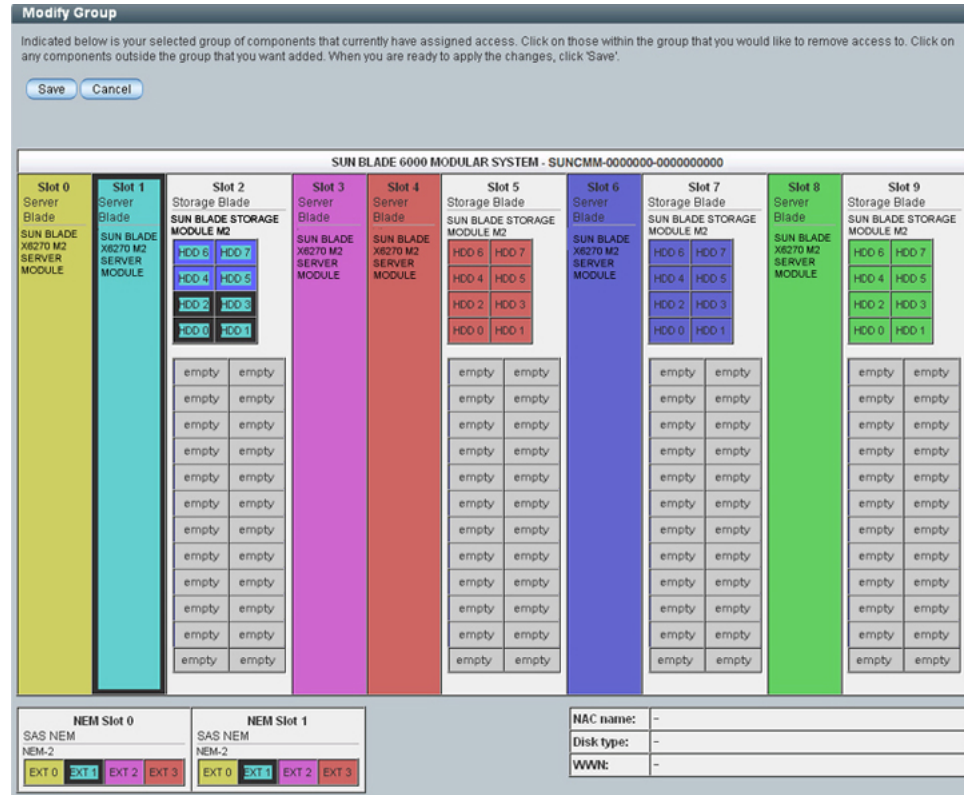
The Sun Blade Zone Manager highlights the storage assigned to the blade storage group in the Zoning Config dialog.



- 4. To modify the storage resources assigned to a selected blade storage group, click **Modify Group**.
The Sun Blade Zone Manager highlights the selected blade storage group (which includes the storage resources currently assigned to the CPU blade server).
- 5. Perform one or more of the following storage modifications to the selected group:

- To remove storage resources allocated to a selected blade storage group, click on the resources that you want to remove.

Example: The following illustration depicts HDD 4-7 as selected resources to be removed from the CPU blade server in slot 1.



- To assign additional storage resources to a blade storage group, click on any storage resources outside the color-coded group that you want to add.
6. To apply the allocation modifications made to the selected blade storage group, click Save.
 7. Back up the saved the recently modified resource allocations.

Related Information

- [“Important SAS Zoning Allocations Considerations ” on page 341](#)
- [“Backing Up and Recovering SAS-2 Zoning Assignments” on page 342](#)
- [“View and Modify Existing Storage Allocations \(CLI\)” on page 365](#)
- *Sun Blade 6000 Modular System Documentation*

▼ View and Modify Existing Storage Allocations (CLI)

Before You Begin

- Ensure that your chassis hardware configuration meets the requirements in [“Chassis Hardware Requirements” on page 343](#).
- Admin (a) role privileges in Oracle ILOM are required to view and modify the Sun Blade Zone Manager properties.
- The Sun Blade Zone Manager must be enabled in Oracle ILOM.

1. Access the Sun Blade Zone Manager from the CLI.

See [“Access and Enable Sun Blade Zone Manager ” on page 343](#).

2. To view storage resources allocated to a CPU blade server, perform one of the following.

- **To view the storage allocations for a CPU blade server, use the `show` command followed by the `/STORAGE/sas_zoning/BLn` target. For example:**

```
-> show /STORAGE/sas_zoning/BL0
```

Targets:

```
0      (/CH/BL2/HDD0)
1      (/CH/BL2/HDD1)
```

In this example, the HDD0 and HDD1, which are currently installed in the storage blade server in chassis slot 2, are allocated to the CPU blade server in chassis slot 0.

- **To view where a storage blade resource is allocated, use the `show` command followed by `/STORAGE/BLn/HDDn` target. For example:**

```
-> show /STORAGE/BL2/HDD0
```

```
Targets:  
  0      (/CH/BL0)
```

```
-> show /STORAGE/BL2/HDD1
```

```
Targets:  
  0      (/CH/BL0)
```

In this example, the resources HDD0 and HDD1, which are installed in the storage blade server in chassis slot 2, are assigned to the CPU blade server in chassis slot 0.

3. To modify the storage allocations, perform one of the following methods:

Method 1: Add or unassign storage resources per CPU blade server.

- To assign a storage resource to a CPU blade server, type:

```
-> cd /STORAGE/sas_zoning/BLn -> set add_storage_access=path_to_storage_device
```

Where *BLn* is the CPU blade server chassis slot location, and *path_to_storage_device* is the path to the storage blade resource.

- To unassign a storage resource from a CPU blade server, type:

```
-> cd /STORAGE/sas_zoning/BLn -> set remove_storage_access=path_to_storage_device
```

Where *BLn* is the CPU blade server chassis slot location, and *path_to_storage_device* is the path to the resource on the storage blade server. For example, */CH/BL1/HDD0*.

Method 2: Add or unassign server blade access to storage device.

- To assign a CPU blade server to a storage resource, type:

```
-> cd /STORAGE/sas_zoning/BLn/HDDn  
-> set add_host_access=path_to_blade_server
```

- To unassign a host server blade access to a storage device, type:

```
-> cd /STORAGE/sas_zoning/BLn/HDDn  
-> set remove_host_access=path_to_blade_server
```

Where *BLn* is the storage blade server chassis slot location, *HDDn* is the storage resource slot location, and *path_to_blade_server* is the chassis slot location for the CPU blade server that you want the resource assigned or unassigned. For example, */CH/BL0*.

Note - You can also add or unassign multiple storage devices in a single command line. To do so, specify the full path to the resource and separate each resource with a comma (no space). For example: `-> set add_storage_access=/CH/BL1/HDD0,/CH/BL1/HDD1`

4. Back up the blade storage group assignment.

Related Information

- [“Important SAS Zoning Allocations Considerations ” on page 341](#)
- [“Backing Up and Recovering SAS-2 Zoning Assignments” on page 342](#)
- [“Manually Create SAS-2 Zoning Allocations \(CLI\)” on page 356](#)
- *Sun Blade 6000 Modular System Documentation*

Resetting Sun Blade Zone Manager Allocations to Factory Defaults

To erase all saved Sun Blade Zone Manager chassis storage allocations and to start the Sun Blade Zone Manager from factory defaults, perform one of the following procedures.

- [“Reset Zoning Allocations to Factory Defaults \(Web\) ” on page 367](#)
- [“Reset Zoning Allocations to Factory Defaults \(CLI\) ” on page 368](#)

▼ Reset Zoning Allocations to Factory Defaults (Web)

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify Sun Blade Zone Manager properties.



Caution - Use this procedure only if you want to erase all currently saved SAS zoning allocations in Oracle ILOM.

1. **To access the Sun Blade Zone Manager page in the CMM web interface, click System Management > SAS Zoning.**

If the Sun Blade Zone Manager state is enabled, a Reset All button appears in the Zoning Reset section of the Sun Blade Zone Manager page.

2. **To erase all saved resource allocations and reset the Sun Blade Zone Manager to factory defaults, click Reset All.**

▼ Reset Zoning Allocations to Factory Defaults (CLI)

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify Sun Blade Zone Manager properties.



Caution - Use this procedure only if you want to erase all currently saved SAS zoning allocations in Oracle ILOM.

1. **Navigate to `/STORAGE/sas_zoning` in the CMM CLI by using the following command:**
2. **To erase all saved resource allocations and reset the Sun Blade Zone Manager to factory defaults, type:**

```
-> cd /STORAGE/sas_zoning
```

```
-> set reset_access_action=true
```

If the Zone Manager is disabled, you will get the following warning:

```
set: The CMM is not the SAS Zone Manager
```

If you receive this message, enable Zone Manager and re-issue the reset command. For details, see [“Access and Enable Sun Blade Zone Manager” on page 343](#).

Resetting the Zoning Password to Factory Default for Third-Party In-Band Management

If you are managing storage allocations for chassis-level storage devices using a third-party in-band zone management application and you need to reset the zoning management password to the factory default, perform one of the following procedures.

- [“Reset the Zoning Password \(Web\)” on page 368](#)
- [“Reset the Zoning Password \(CLI\)” on page 369](#)

▼ Reset the Zoning Password (Web)

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify Sun Blade Zone Manager properties.



Caution - Use this procedure only if you are not using Oracle ILOM Zone Manager, and you are using a third-party in-band management application to manage the chassis storage allocations.

1. **To verify that the Sun Blade Zone Manager state is disabled in the CMM web interface, click System Management > SAS Zoning.**

The Sun Blade Zone Manager page appears.

If the Sun Blade Zone Manager is disabled, an option for resetting the password appears in the In-band Zoning Manager section.

2. **To reset the zoning password to the default value (all zeros), click Reset.**

▼ Reset the Zoning Password (CLI)

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify Sun Blade Zone Manager properties.



Caution - Use this procedure only if you are not using Oracle ILOM Zone Manager, and you are using a third-party in-band management application to manage the chassis storage allocations.

1. **Navigate to `/STORAGE/sas_zoning` using the following command:**

```
-> cd /STORAGE/sas_zoning
```

2. **To reset the current zoning password, type:**

```
-> set reset_password_action=true
```

The password is set to the default (all zeros).

Index

A

alerts

- specifying destination, 262
- types of levels, 262
- types supported, 262

C

CLI

- Sun Blade Zone Manager, 340
- using to create Sun Blade Zone Manager chassis storage configuration, 356

D

- Detailed Setup for Sun Blade Zone Manager, 347
- dnssec-keygen, 138
- Dynamic DNS
 - Debian r4.0 environment, 138
 - dnssec-keygen, 138
 - operating systems supported, 138

I

- init.d script, 140
- IPMI PET alerts, 262

L

- log in to ILOM
 - using root user account password, 39

N

- nslookup, 140

Q

- Quick Setup for Sun Blade Zone Manager, 345

S

- saving a storage access configuration, 341
- SNMP Trap alerts, 262
- storage access configuration table in Sun Blade Zone Manager, 358
- Sun Blade Zone Manager
 - CLI, 340
 - creating the chassis storage access configuration
 - using CLI, 356
 - using detailed setup, 347
 - using quick setup, 345
 - resetting a zoning configuration
 - using web interface, 367
 - resetting the zoning password
 - using web interface, 369
 - saving a storage access configuration, 341
 - storage access configuration table, 358
 - view and modify storage configuration
 - using the web interface, 361, 365, 367, 368, 368

T

- topic guidelines, 317, 331

W

web interface

- recovering a storage zoning configuration, 367
- resetting the zoning password, 369
- using to view and modify storage configuration, 361, 365, 367, 368, 368