Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 5.0.x

E95138-09
October 2023

Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 5.0.x,

E95138-09

Primary Author: Cheryl Smith, Heidi Hall

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

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

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

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

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

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

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

Contents

4 Modifying Default Settings for Network Deployment and Administration

5 Using Remote KVMS Consoles for Host Server Redirection

6 Using the Oracle ILOM Remote System Console or Storage Redirection CLI

7 Using the Oracle ILOM Remote System Console Plus

8 Configuring Host Server Management Actions

9 Configuring Alert Notifications, Service Requests, or Remote Logging

10 Setting System Management Power Source Policies and Device Monitoring

11 Setting Power Alert Notifications and Managing System Power Usage

12 Performing Oracle ILOM Maintenance and Configuration Management Tasks

1
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/E95134_01/index.html .

Feedback

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

2

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
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
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
Refer to this section for information on how to locate guidelines for enhancing Oracle ILOM security.	• Configuring Oracle ILOM for Increased Security

Related Information

- Oracle Server Installation Guide and Administration Guide
- Checklists for Keeping Oracle ILOM Secure

Establishing a Management Connection to Oracle ILOM

The Oracle ILOM firmware arrives preconfigured on your Oracle server 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
- Management Services and Network Default Properties

Choosing and Configuring a Management Connection to Oracle ILOM

Oracle ILOM supports the following management connections:

- Dedicated Network Management Connection (Default)
- Sideband Network Management Connection
- Dedicated Local Management Connection
- Dedicated Interconnect SP Management Connection

Dedicated Network Management Connection (Default)

All Oracle servers 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 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.
- 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.

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

1. On the physical server 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.

   > **Note:**
   >
   > When an active LAN connection is attached to the NET MGT port on the managed server, Oracle ILOM automatically detects an IP address for the SP from the IP routing device on your network. For guidelines for determining the IP address assigned to the Oracle ILOM SP, see Usage Guidelines for IP Network Management Address.

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, perform the following steps using the applicable user interface.

User Interface	Step	Task: Verify or reset default management port property for SP
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: • `show /SP/network` For login instructions, see Log In to the Oracle ILOM SP.
	2:	Verify that the `/network` output displays the default Management Port property for the SP, for example: • SP output: `managementport=MGMT`
	3:	If necessary, reset the default Management Port property for the SP. For SP, type: `set /SP/network pendingmanagementport=MGMT commitpending=true`
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.
	2:	In the Network Settings page, verify that the Management Port list box for the SP is set to `MGMT`.
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
- Setting Up and Maintaining User Accounts

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
- Sideband Management Network Connectivity Considerations

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.
- 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)

    - Dedicated Local Management Connection
  - You should have logged in to Oracle ILOM. For instructions, see Logging In to Oracle ILOM Server SP..
  - 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
- Usage Guidelines for IP Network Management Address
- Modifying Default Connectivity Configuration Properties
- Recommended Practice for Spanning Tree Configurations
- Setting Up and Maintaining User Accounts
- Assigning System Identification Information

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 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.
  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.
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, press Enter.

Related Information

- Management Services and Network Default Properties
- Modifying Default Connectivity Configuration Properties
- Assignable Oracle ILOM User Roles
- Serial Management Port Owner
- Assigning System Identification Information

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
- Manually Configure the Local Interconnect
- Host OS Interconnect Guidelines for Manual Configuration
- Oracle ILOM SP Interconnect Properties

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.

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.

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.

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.
- 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.

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

   a. Review Oracle ILOM SP Interconnect Properties.

   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.

   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	i. 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. ii. 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. iii. 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 . **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.

Oracle ILOM Interface	**Steps:**

CLI	i. Navigate to the `/network/interconnect` working directory on the managed server.
	For example:
	From a single server SP CLI, type: `cd /SP/network/interconnect`
	From a multi-domain server SP CLI, type:`cd /Servers/PDomains/PDomain_` *n* `/SP/network/interconnect`
	ii. To disable the `hostmanaged` 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.
	iii. Set the `allowed_services` communication property. For further configuration details, see Oracle ILOM SP Interconnect Properties
	iv. 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.

Related Information

- Host OS Interconnect Guidelines for Manual Configuration
- Oracle ILOM SP Interconnect Properties
- Logging In to Oracle ILOM Server SP
- Oracle ILOM Deployment Practices for Increasing Security
- 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 2-1 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 `ilomconfig` tool. This tool is included in the Oracle Hardware Management Pack software distribution.
	Note: As an alternative to using the ilomconfig tool, you can use OS networking commands to configure the internal Ethernet-over-USB connection point addresses.
	3. In the ilomconfig tool, do one of the following:
	• Manually set the connection point addresses for the internal Ethernet-over-USB interface:
	`ilomconfig enable interconnect --spipaddress=x.x.x.x --netmask=x.x.x.x --hostipaddress=x.x.x.x`
	-or-
	• Manually set the default connection point addresses for the internal Ethernet-over-USB interface:
	`ilomconfig enable interconnect`

Table 2-1 (Cont.) Host OS Interconnect Manual Configuration Guidelines

Operating System	Manual Host OS Interconnect Guidelines
Solaris	1. Ensure that the internal Ethernet-over-USB device is automatically discovered by Oracle Solaris. 2. In the ilomconfig tool, do one of the following: **Note:** The ilomconfig tool is part of Oracle Solaris, no installation is required. • Manually set the connection point addresses for the internal Ethernet-over-USB interface: `ilomconfig enable interconnect --spipaddress=x.x.x.x --netmask=x.x.x.x --hostipaddress=x.x.x.x` -or- • Manually set the default connection point addresses for the internal Ethernet-over-USB interface: `ilomconfig enable interconnect`

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 2-2 Oracle ILOM SP Interconnect Properties

<table>
<tr><th>Property</th><th>Default Value</th><th>Description</th></tr>
<tr><td>Host Managed
(hostmanaged=|)</td><td>Enabled (True)</td><td>*Enabled (True)* | *Disabled (False)*
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
set /SP/network/interconnect hostmanaged=*true*|*false*
Multi-Domain SP CLI Syntax
set /Servers/PDomains/PDomain_*n*/SP/network/interconnect hostmanaged=*true*|*false*</td></tr>
<tr><td>State
(state=)</td><td>Disabled</td><td>*Enabled* | *Disabled* (default)
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.
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*
Multi-Domain SP CLI Syntax
set /Servers/PDomains/PDomain_*n*/SP/network/interconnect state=*enabled*|*disabled*</td></tr>
</table>

Table 2-2 (Cont.) Oracle ILOM SP Interconnect Properties

Property	Default Value	Description
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 The Allowed Services property is available for configuration as of Oracle ILOM firmware version 3.2.6. **Note:** 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** Single SP CLI example: `set /SP/network/interconnect allowed_services=`*`fault-transport, http, https, ipmi, snmp, ssh`*
Save (`commitpending=`*true*|*false*)	(Not Applicable)	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 (`spmacaddress=`)	Read-only	The read-only property for the Service Processor MAC Address displays the MAC address that is assigned to the Oracle ILOM SP.

Table 2-2 (Cont.) Oracle ILOM SP Interconnect Properties

Property	Default Value	Description
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	(Not Applicable)	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`/network/interconnect` *property_name* **Example:** `help /SP/network/interconnect hostmanaged`
More details ... (web help)	(Note Applicable)	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.

- Management Services Enabled by Default Management Services Enabled by Default
- Network Connectivity Properties Enabled by Default Network Connectivity Properties Enabled by Default

Table 2-3 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	Web Server Configuration Properties
Web Server: State	• HTTPS, Enabled	443	Web Server Configuration Properties

Table 2-3 (Cont.) Management Services Enabled by Default

Management Access	Default Properties	Service Port	To modify configurable properties, see;
Web Server: SSL	Later firmware versions of Oracle ILOM) • TLS v1.2 Enabled • Default SSL certificate • Default SSL self-signing private key	-	SSL Certificate and Private Key Configuration Properties for HTTPS Web Server
IPMI: State	• Enabled	623	IPMI Service Configuration Properties **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	SNMP Configuration Properties
Single Sign On	• Enabled	11626	Single Sign-On Service (Enabled by Default)
Secure Shell (SSH)	• Enabled • RSA and DSA Key Generation	22	SSH Server Configuration Properties
Remote KVMS Redirection (video, keyboard, mouse, and storage)	• Enabled	5120-5123, 5555, 5556, 7578, 7579	Using Remote KVMS Consoles for Host Server Redirection
Service tag[1]	• Enabled	6481	Servicetag Service Configuration Properties

[1] 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.

Table 2-4 Network Connectivity Properties Enabled by Default

Network Connectivity Property	Default Value	To modify configurable properties, see:
Network: State	• Enabled	Network Connectivity Standard Configuration Properties
IPv4: Mode	• DHCP, enabled	
IPv6: State	• Enabled	Network Connectivity Standard Configuration Properties
IPv6: Mode	• Auto-Config, Stateless	
Management Port:	• Dedicated Network Management (MGMT)	Network Connectivity Standard Configuration Properties

Table 2-4 (Cont.) Network Connectivity Properties Enabled by Default

Network Connectivity Property	Default Value	To modify configurable properties, see:
Local Host Interconnect	• Host Utilities Managed: Enabled • State: Disabled	Dedicated Interconnect SP Management Connection
DNS	• Auto DNS via DHCP, Enabled	DNS Configuration Properties
Serial Port	• Owner: Service Processor • Baud Rate: 9600 • Host Flow Control: None	Serial Port Configuration Properties
User Authentication[1]	• Root user account: root • Root password: `changeme` • Permitted local accounts: Up to 10 customer-configurable user accounts • Single Sign On: Enabled for remote KVMS.	Managing User Credentials

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

Logging In to Oracle ILOM Server SP

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
- Usage Guidelines for IP Network Management Address
- Preconfigured User Accounts Enabled by Default
- Supported Web Browsers for Oracle ILOM

Log In to the Oracle ILOM SP

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.
- 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. For information about how to create user accounts in Oracle ILOM, see Managing User Credentials .

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 `root` for user name and `changeme` for password.
Web browser	a. Type `http://` *ILOM_SP_ipaddress* 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. b. Log in to the Oracle ILOM web interface by specifying a valid Oracle ILOM use r name and password. For example: Type `root` for user name and `changeme` for password. The Oracle ILOM Summary page appears.
CLI secure shell	a. To establish an SSH session to the Oracle ILOM CLI, open a terminal window. b. To log in to Oracle ILOM using the default `root` account, type: `$ ssh root@` *ILOM_SP_ipaddress* Oracle ILOM prompts you for the `root` password. c. At the Password prompt, type `changeme`. The Oracle ILOM CLI prompt appears (`->`).

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
- Default Timeout for CLI and Web Sessions
- Modifying Default Management Access Configuration Properties
- Management of Banner Messages at Log-In
- Setting Up and Maintaining User Accounts
- Password Recovery for Default root Account
- Setting Up a Management Connection to Oracle ILOM and Logging In
- Using Remote KVMS Consoles for Host Server Redirection
- Viewing System Inventory, Health, and Performing Service and Management Actions
- CLI Reference for Mapping Management Tasks to CLI Targets
- Updating Oracle ILOM Firmware

Usage Guidelines for IP Network Management Address

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

Table 2-5 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.Log in to Oracle ILOM 2. 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. 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 *must be enclosed* in brackets to work correctly. For example: `https://[` *ipv6address* `]` - When establishing an Oracle ILOM CLI session using SSH, the IPv6 address *should not be enclosed* in brackets. For example: `ssh root@` *ipv6address* - When transferring a file using the CLI `load -source` command and `tftp`, the IPv6 address *must be enclosed* 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 2-6 Local User Accounts Enabled by Default

Preconfigured User Account	Default Login Properties	Description	To modify, see:
`root`	• Username: `root` • Password: `changeme`	The Oracle ILOM `root` user account is a persistent local user account that is available on all Oracle ILOM interfaces[1], unless, you choose to delete the persistent `root` user account. **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, you should either: • Modify the default `root` password (`changeme`) provided on each Oracle ILOM service processor (SP). - or - • Delete the preconfigured `root` account provided on the Oracle ILOM SP. 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.	Managing User Credentials
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. **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**: • Recover Preconfigured root Account or root Account Password (CLI only) • (Physical Presence) Assigning System Identification Information	Password Recovery for Default root Account

[1] 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 tested web browsers on the SP, 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 2-7 Supported Web Browsers for Oracle ILOM

Operating System	Web Browser
Oracle Solaris 11.3	• Mozilla Firefox 45.2
Oracle Linux 7, Red Hat Enterprise Linux 7, SuSE Linux Enterprise 12, Ubuntu Linux LTS 14	• Mozilla Firefox 60.6.1esr
Microsoft Windows 10, Microsoft Windows 11 **Note**: Given that Microsoft has deprecated Internet Explorer 11, Mircrosoft Edge is currently supported in all Oracle ILOM firmware releases as a web client. For more information about Oracle's technical support policy concerning web browser support, see Oracle Software Web Browser Support Policy.	• Google Chrome v103 • Microsoft Edge v103 • Mozilla Firefox v102
Apple Mac OS X[1] [2]	• Safari 11.1

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

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

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 .

3 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
Refer to this section for requirements and instructions for configuring local user accounts in Oracle ILOM.	• Configuring Local User Accounts
Refer to this section for information about configuring the Password Policy for all local user accounts.	• Managing Password Policy Restrictions for Local Users
Refer to this section for requirements and instructions for configuring Oracle ILOM as an Active Directory client.	• Configuring Active Directory
Refer to these sections for requirements and instructions for configuring Oracle ILOM as an LDAP/SSL client or LDAP client.	• Configuring LDAP/SSL • Configuring LDAP
Refer to this section for requirements and instructions for configuring Oracle ILOM as a RADIUS client.	• Configuring RADIUS

Related Information

- Oracle ILOM Deployment Practices for Increasing Security
- Preconfigured User Accounts Enabled by Default

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
- Assignable Oracle ILOM User Roles
- Single Sign-On Service (Enabled by Default)
- Maximum Number of User Sessions Supported
- Manage User Authenticated Sessions per Managed Device
- CLI Authentication Using Local User SSH Key

- Security Action: Change Default root Account Password
- Password Recovery for Default root Account
- Supported File Transfer Methods

Supported User Authentication Configuration Options

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

Table 3-1 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). • Configurable user role privileges granting either read-only or read and write access to discrete Oracle ILOM features (see Assignable Oracle ILOM User Roles). • Secure user authentication and authorization for local and remote management. • Oracle ILOM user credentials are maintained separately for each SP. For additional information about configuring local user accounts in Oracle ILOM, see Configuring Local User Accounts .
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 in local network environment). • Enables authenticated Oracle ILOM users to have access to all Oracle ILOM instances. • Enables system administrators to configure user authentication rules for using features within Oracle ILOM.

Table 3-2 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 .

Table 3-2 (Cont.) Supported Authentication Directory Services

Authentication Service	Description
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.
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.
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 .

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:

- Privileges Granted by a User Profile Privileges Granted by a User Profile
- Privileges Granted by Individual User Roles Privileges Granted by Individual User Roles

Table 3-3 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 Privileges Granted by Individual User Roles.
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 Privileges Granted by Individual User Roles.
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) **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 Privileges Granted by Individual User Roles.

Table 3-4 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, 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. This service enables Oracle ILOM 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.

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/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
(`/sso state=`)
	Enabled	*Enabled |Disabled*
		CLI SSO State Syntax Examples:
		Single server SP:
		`set /SP/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. 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/sessions/`**
- **Web: ILOM Administration > User Management > Active Sessions**
- **User Role: Admin (a) role is required to terminate a user session.**

Property	Description

Active Sessions
(`/session`s)
	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, type:
	`show /SP/sessions`
	• From a multi-domain server SP, type:
	`show /Servers/PDomains/PDomain_` *n* `/SP/sessions`
	Possible property values shown for `/session type=` *shell* | *console* | *web* | *snmp* |*video redirection* | *serialredirection*
	• 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 `/session mode=` *normal* | *service* | *escalation*

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, type: `delete /SP/sessions/`*n* A confirmation message appears, type Y to continue or N to cancel the action. • From a multi-server SP, type: `delete /Servers/PDomains/PDomain_` *n* `/SP/sessions/` *n* 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.

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 3-5 Adding or Removing Public SSH Key File per Local User Account

User Interface Configurable Target:

- **CLI: `/SP/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
Key Upload - File Transfer Options (`set load_uri=`)	*Browser|TFTP|SFTP|SCP|HTTP|HTTPS|Paste* For a description of each file transfer method, see File Transfer Methods .
Add SSH Key (`/ssh/keys/1`)	**CLI Add SSH Key Syntax:** **set /SP/users/** *user_account_name* **/ssh/keys/1 load_uri=** *transfer_method://username:password@ipaddress_or_hostname/directorypath/filename* **Example:** set /SP/users/adminuser/ssh/keys/1 load_uri=scp://adminuser:userpswd@198.51.100.4/keys/sshkey_1.pub **Note:** The maximum SSH key size for RSA is 8192 bits.
Delete SSH Key (clear action=true)	**CLI Delete SSH Key Syntax**: `set /SP/users/user_account_name/ssh/keys/1 clear_action=true` 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 View, Modify, or Remove User Account.

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 3-6 Recover Preconfigured `root` Account or `root` Account Password (CLI only)

Prerequisites	Instructions

• Local Serial Management Connection to Oracle ILOM
• Physical presence at managed server, if Physical Presence State is enabled (default)
	1. Establish a local serial management connection to Oracle ILOM and log in to Oracle ILOM using the `default` user account. For example:
	`SUNSP-0000000000 login: default`
	`Press and release the physical presence button. Press return when this is completed...`
	2. 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.
	3. Return to your serial console and press Enter.
	You will be prompted for a password.
	4. Type the password for the `default` user account: **defaultpassword**.
	5. 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
- Configure a Dedicated Local Management Connection to Oracle ILOM
- (Physical Presence) Assigning System Identification Information
- Managing Password Policy Restrictions for Local Users
- Create User Account and Assign User Roles
- View, Modify, or Remove User Account

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 3-7 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.
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 `dump_uri` or `load_uri` 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.

- Create User Account and Assign User Roles Create User Account and Assign User Roles
- View, Modify, or Remove User Account 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.

Table 3-8 Create User Account and Assign User Roles

<table>
<tr><td colspan="2"><b>User Interface Configurable Target:</b>
• <b>CLI: <code>/SP/users/</code></b>
• <b>Web: ILOM Administration > User Management > User Accounts</b>
• <b>User Role: User Management (u) (required to create user accounts).</b></td></tr>
<tr><th>Property</th><th>Description</th></tr>
<tr><td>Users &gt; Add
(<i>user_name</i> password= role =)</td><td><i>user_name</i> |Password=|Role= <i>administrator |operator|advanced</i> (a|u|c|r|o|s)
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.
<b>CLI Create User Syntax</b>:
create / <i>SP</i>|/users/ <i>user_name_for_account</i> password= <i>password_for_account</i> role= <i>administrator|operator|a|u|c|r|o|s</i>
<b>Example Syntax:</b>
<code>create /SP/users user5 password=administrator role=aucr</code>
<b>Note</b>. 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.</td></tr>
<tr><td>Save</td><td><b>Web interface</b> – To apply changes made to properties within the Add User dialog, you must click Save.</td></tr>
</table>

Table 3-9 View, Modify, or Remove User Account

User Interface Configurable Target:

- **CLI: `/SP/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.**

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td>Users
(<code>/users</code>)</td><td>View local user accounts configured in Oracle ILOM.
<b>CLI View Users Syntax</b>:
<code>show /SP/users</code> <b>Example syntax:</b>
<code>show /SP/users</code></td></tr>
<tr><td>Users > Edit
(<code>/<i>user_name</i> password</code>= role=)</td><td>Password=<i>user_configurable</i>|role=<i>administrator</i> |<i>operator</i>|<i>advanced</i> (a|u|c|r|o|s)
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 <code>root</code> user.
<b>Web interface</b> – Click Save to apply the changes made within the Edit User dialog.
<b>CLI Edit User Account Syntax</b>:
<code>set /SP/users</code> <i>user_name</i> <code>password=<i>assign_new_password</i> role=</code> <i>administrator</i>|<i>operator</i>|a|u|c|r|o|s
<b>Example Syntax</b>: <code>set /SP/users user5 password=administrator role=auco</code></td></tr>
<tr><td>Users > Delete
(<code>/<i>user_name</i></code>)</td><td>Specify the name of the user account to delete. When prompted, confirm the action.
<b>Note:</b>
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.
<b>CLI Delete User Account Syntax:</b>
<code>delete /SP/users/</code><i>user_name</i>
<b>Example Syntax:</b>
<code>delete /SP/users/user5</code></td></tr>
</table>

Related Information

- Managing Password Policy Restrictions for Local Users
- Privileges Granted by a User Profile
- View, Modify, or Remove User Account
- Local User Accounts Enabled by Default
- Recover Preconfigured root Account or root Account Password (CLI only)
- CLI Authentication Using Local User SSH Key
- Security Action: Change Default root Account Password

- Create User Account and Assign User Roles

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 and Account Locking Properties for Local Users
- Password Policy Management Properties and Defaults

Modify Password Policy Restrictions and Account Locking Properties 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. Configure password restrictions and account locking properties as required. For a description of each property, see Password Settings Configuration Properties.

     b. 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.
        ```

     c. 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: Configure Password Restrictions:

     a. Type the following command string to configure the password policy settings:
        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 setting, see Password Settings Configuration Properties.

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.

3. CLI: Configure the Account Locking Properties

a. Type the following command string, then press Enter to configure the Account Locking properties.
set /SP/preferences/password_policy/account_lockout [state= *enabled* | *disabled*] [attempts = *n*] [delay= *enabled* | *disabled*] [delay_time = *n*]

where:

- state = Account Locking state (enabled (default) | disabled)
- attempts = Maximum attempts (12 Maximum Attempts (default) | User-Specified Maximum Attempts (1 to 12)
- delay = Enable after Delay (enabled (default) | disabled).
- delay_time = Delay Time (12 Hours 0 Minutes (default) | User-Specified Hours (1 to 12) and Minutes (0 to 59)).

For a description of each account locking property, see Configure Account Locking Properties.

Related Information:

- Securing Oracle ILOM User Access
- Post Deployment Considerations for Securing User Access
- Security Action: Change Default root Account Password
- Password Recovery for Default root Account
- Configuring Local User Accounts

Password Policy Management Properties and Defaults

The following tables describe the CLI and web properties for the Oracle ILOM Password Settings and Account Locking properties.

- Password Settings Configuration Properties
- Configure Account Locking Properties

Table 3-10 Password Settings Configuration Properties

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 (`u`)	Disabled, no restrictions	Disabled (no restrictions) | Enabled (requires at least 1), 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.

Table 3-10 (Cont.) Password Settings Configuration Properties

Property	Default	Description
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.

Table 3-11 Configure Account Locking Properties

Property	Default	Description
Account Locking (state =)	Enabled	Enabled | Disabled • Enabled — Select the Account Locking Enabled check box to enable the account lockout mode. When the account lockout mode is enabled, any user that exceeds the specified maximum number of login attempts will be locked out of their account. • Disabled — Clear the Account Locking Enabled check box to disable the account lockout mode. When the account lockout mode is disabled, all user failed login attempts are cleared. Note that a warning message will appear prompting the user to confirm this action.
Maximum Attempts (attempts =)	12	12 Maximum Attempts (default) | User-Specified Maximum Attempts (1 to 12) Enter the maximum number of failed login attempts a local user must not exceed before their account is locked.
Enable After Delay (delay =)	Enabled	Enabled (default) | Disabled • Enabled — Select the Enable After Delay check box to permit the password policy to unlock a user account after the specified time elapsed (hours and minutes specified in the Delay Time property). • Disabled — Clear the Enable After Delay check box to disable the unlocking of local users accounts.
Delay Time (delay_time =)	12 Hours and 0 Minutes	12 Hours and 0 Minutes (default) | User-Specified Hours (1 to 12) and Minutes (0 to 59) When the Enable After Delay check box is selected, enter the maximum time during which a local user account will remain locked until the password policy is permitted to unlock the user account.

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:

- Enabling Active Directory Authentication Enabling Active Directory Authentication

- Uploading or Removing an Active Directory Certificate File Uploading or Removing an Active Directory Certificate File
- Optionally Configuring Active Directory Groups Optionally Configuring Active Directory Groups
- Configuring Active Directory User Domains Configuring Active Directory User Domains
- Optionally Configuring Active Directory Alternate Servers Optionally Configuring Active Directory Alternate Servers
- Optionally Editing DNS Locator Queries Optionally Editing DNS Locator Queries
- Guidelines for Troubleshooting Active Directory Authentication Guidelines for Troubleshooting Active Directory Authentication

Table 3-12 Enabling Active Directory Authentication

User Interface Configurable Target:

- **CLI: `/SP/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
State (`state=`)	Disabled	*Disabled* |*Enabled* 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. **CLI State Syntax**: `set /SP/clients/activedirectory/ state=`*`disabled`*`|`*`enabled`*

Table 3-12 (Cont.) Enabling Active Directory Authentication

User Interface Configurable Target:

- **CLI: `/SP/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
Roles (`defaultrole=`)	None (server authorization)	*Administrator |Operator |Advanced |None (server authorization)* 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/clients/activedirectory/ defaultrole=`*`administrator`*`|`*`operator`*`|`*`a`*`|`*`u`*`|`*`c`*`|`*`r`*`|`*`o`*`|`*`s`*`|`*`none`* **Related Information:** • Privileges Granted by a User Profile • Privileges Granted by a User Profile • Optionally Configuring Active Directory Groups
Address (`address=`)	0.0.0.0	*IP address*| *DNS host name* (Active Directory Server) 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/clients/activedirectory/ address=`*`active_directory_server ip_address`*`|` *`active_directory_server_dns_host_name`* **Related Information:** • DNS Configuration Properties

Table 3-12 (Cont.) Enabling Active Directory Authentication

User Interface Configurable Target:

- **CLI: `/SP/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 (`port=`)	0 (Auto-select)	*0 Auto-select* | *Non-standard TCP 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/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/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. The Active Directory server certificate must be loaded prior to enabling the Strict Certificate Mode property. **CLI Strict Certificate Mode Syntax**: `set /SP/clients/activedirectory/ strictcertmode=`*`disabled`*`|`*`enabled`* **Related Information**: • Uploading or Removing an Active Directory Certificate File

Table 3-12 (Cont.) Enabling Active Directory Authentication

User Interface Configurable Target:

- **CLI: `/SP/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
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. **CLI DNS Locator Mode Syntax**: `set /SP/clients/activedirectory/ dnslocatorqueries/1=disabled|enabled` **Related Information**: • Optionally Editing DNS Locator Queries
Expanded Search Mode (`expsearchmode=`)	Disabled	*Disabled* | *Enabled* 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/clients/activedirectory/ expsearchmode=disabled|enabled`
Strict Credential Error Mode (`strictcredentialerrormode=`)	Disabled	*Disabled* | *Enabled* 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/clients/activedirectory/ strictcredentialerrormode=disabled|enabled` **Related Information**: • Uploading or Removing an Active Directory Certificate File
Log Detail (`logdetail=`)	None	*None* | *High* | *Medium* | *Low* |*Trace* 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**: `set /SP/clients/activedirectory/ logdetail=none|high|medium|low|trace`
Save		**Web interface** – To apply changes made to properties within the Active Directory Settings page, you must click Save.

Table 3-13 Uploading or Removing an Active Directory Certificate File

User Interface Configurable Target:

- **CLI: `/SP/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	*Certificate present |Certificate not present* The Certificate File Status property indicates whether an Active Directory certificate has been uploaded to Oracle ILOM. The Active Directory certificate file must be uploaded to Oracle ILOM prior to enabling the Strict Certificate Mode property. **CLI Certificate Show Syntax**: `show /SP/clients/activedirectory/cert`
File Transfer Method	Browser (web interface only)	*Browser|TFTP|FTP|SCP|Paste* For a detailed description of each file transfer method, see File Transfer Methods .
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=file_transfer_method://host_address/file_path/filename`

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 /SP/clients/activedirectory/cert clear_action=true`
		-or-
		`reset /SP/clients/activedirectory/cert`
		When prompted, type `y` to delete or `n` to cancel the action.

Table 3-14 Optionally Configuring Active Directory Groups

User Interface Configurable Target:

- **CLI: `/SP/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 /SP/clients/activedirectory/admingroups/n name=string
	Example Syntax:
	`set /SP/clients/activedirectory/admingroups/1/`
	`name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com`
	`Set 'name' to`
	`'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com'`

Table 3-14 (Cont.) Optionally Configuring Active Directory Groups

User Interface Configurable Target:

- **CLI: `/SP/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

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.
	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:
	`set /SP/clients/activedirectory/operatorgroups/n name=string`
	Example Syntax:
	`set /SP/clients/activedirectory/operatorgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com`
	`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:** `set /SP/clients/activedirectory/hostgroups/n/ name=string hosts=string roles=string` 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 available for the Oracle server.

Table 3-14 (Cont.) Optionally Configuring Active Directory Groups

User Interface Configurable Target:

- **CLI: `/SP/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

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 Enabling Active Directory Authentication .
	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: *administrator* |*operator*|*advanced* (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:
	`set /SP/clients/activedirectory/customgroups/n name=string roles=administrator|operator|a|u|c|r|o|s`
	Example Syntax:
	`set /SP/clients/activedirectory/customgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com roles=au`
	`Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com'' roles' to 'au'`
	Related Information:
	• Assignable Oracle ILOM User Roles

Save	**Web interface** – To apply changes made to properties in the Admin, Operator, or Custom Group dialogs, you must click Save.

Table 3-15 Configuring Active Directory User Domains

User Interface Configurable Target:

- **CLI: `/SP/clients/activedirectory/userdomains/` *n***
- **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: `<USERNAME>@domain.company.com`
	• DN format: `CN=<USERNAME>,CN=Users,DC=domain,DC=company,DC=com`
	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.
	CLI User Domains Syntax:
	`set /SP/clients/activedirectory/userdomains/n name=string`
	Example 1: `name=CN=<USERNAME>`
	`set /SP/clients/activedirectory/userdomains/1/ name=CN<USERNAME>, OU=Groups, DC=sales, DC-Oracle, DC=com`
	Set 'name' to 'CN=<USERNAME>,OU=Groups,DC=sales,DC=oracle,DC=com'
	Example 2: name=CN=spSuperAdmin
	`set /SP/clients/activedirectory/userdomains/1/ name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com`
	`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 3-16 Optionally Configuring Active Directory Alternate Servers

User Interface Configurable Target:

- **CLI: `/SP/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

Alternate Servers
(/*1*|*2*|*3*|*4*|*5*)
	Oracle ILOM enables a system administrator to configure up to five Active Directory alternate servers.
	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 Enabling Active Directory Authentication
	CLI Alternate Server Address and Port syntax:
	`set /SP/clients/activedirectory/alternateservers/n address=sting port=string`
	CLI Alternate Server Certificate Syntax:
	`show /SP/clients/activedirectory/alternateservers/n/cert`
	`load_uri=file_transfer_method://host_address/file_path/filename`
	`set /SP/clients/activedirectory/alternateservers/n/cert clear_action=true`

Save	**Web interface** – To apply changes made to properties in the Active Directory Alternate Servers dialog, you must click Save.

Table 3-17 Optionally Editing DNS Locator Queries

User Interface Configurable Target:

- **CLI: `/SP/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
(/1)
	_ldap._tcp.gc._msdcs.`<DOMAIN>.<PORT:3269>`	Oracle ILOM enables you to configure up to five DNS Locator Queries.
		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 <PORT:636>. Additionally, you can override the named DNS service for a specific domain by using the <DOMAIN> substitution marker.
		CLI Show and Edit DNS Locator Queries Syntax:
		`show /SP/clients/activedirectory/dnslocatorqueries/1`
		`set /SP/clients/activedirectory/dnslocatorqueries/1 service =` *`string`*
		Example DNS Locator Queries Syntax for `service=string`:
		`service =_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:`*`nnnn`*`>`

DNS Locator Queries (/2)	_ldap._tcp.dc._msdcs`.<DOMAIN>.<PORT:636>`	
Save		**Web interface** – To apply changes made to properties in the Active Directory DNS Locator Queries dialog, you must click Save.

Table 3-18 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:

- Enabling Active Directory Authentication
- Managing Oracle ILOM Log Entries
- Setting ILOM Clock Properties

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:

- Enabling LDAP/SSL Authentication Enabling LDAP/SSL Authentication
- Uploading or Removing an LDAP/SSL Certificate File Uploading or Removing an LDAP/SSL Certificate File
- Optionally Configuring LDAP/SSL Groups Optionally Configuring LDAP/SSL Groups
- Configuring LDAP/SSL User Domains Configuring LDAP/SSL User Domains
- Optionally Configuring LDAP/SSL Alternate Servers Optionally Configuring LDAP/SSL Alternate Servers
- Guidelines for Troubleshooting LDAP/SSL Authentication Guidelines for Troubleshooting LDAP/SSL Authentication

Table 3-19 Enabling LDAP/SSL Authentication

User Interface Configurable Target:

- **CLI: `/SP/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
State (`state=`)	Disabled	*Disabled* |*Enabled* 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 /SP/clients/ldapssl/ state=`*`disabled`*`|`*`enabled`*

Table 3-19 (Cont.) Enabling LDAP/SSL Authentication

User Interface Configurable Target:

- **CLI: `/SP/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
Roles (`defaultrole=`)	None (server authorization)	*Administrator* |*Operator* |*Advanced* |*None* (server authorization) 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. `set /SP/clients/ldapssl/ defaultrole=`*`administrator`*`|`*`operator`*`|`*`a`*`|`*`u`*`|`*`c`*`|`*`r`*`|`*`o`*`|`*`s`*`|`*`none`* **Related Information:** • Privileges Granted by a User Profile • Privileges Granted by Individual User Roles • Optionally Configuring LDAP/SSL Groups
Address (`address=`)	0.0.0.0	*IP address*| *DNS host name* (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**: `set /SP/clients/ldapssl/ address=`*`LDAP/SSL_server ip_address`*`|`*`active_directory_server_dns_host_name`* **Related Information:** • DNS Configuration Properties

Table 3-19 (Cont.) Enabling LDAP/SSL Authentication

User Interface Configurable Target:

- **CLI: `/SP/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
Port (`port=`)	0 Auto-select	*0 Auto-select* | *Non-standard TCP port* 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. 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/clients/ldapssl/ port=`*`number`*
Timeout (`timeout=`)	4 seconds	*4* |*user-specified* 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 /SP/clients/ldapssl/ timeout=`*`number_of_seconds`*
Strict Certificate Mode (`strictcertmode=`)	Disabled	*Disabled* |*Enabled* 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 /SP/clients/ldapssl/ strictcertmode=`*`disabled`*`|`*`enabled`* **Related Information**: • Uploading or Removing an LDAP/SSL Certificate File

Table 3-19 (Cont.) Enabling LDAP/SSL Authentication

User Interface Configurable Target:

- **CLI: `/SP/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
Optional User Mapping (`/optionalUsermapping`)	Disabled	*Disabled* | *Enabled* 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. • 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: `OU={organization},DC={company},DC={com}` • 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: `OU={organization},DC={company},DC={com}` • Bind Password – Set the Bind Password property to a password for the read-only proxy user. **CLI Optional User Mapping Syntax**: `set /SP/clients/ldapssl/optionalUsermapping/ attributeInfo=<string> searchbase=<string> binddn=cn=`*`proxyuser`*`, ou=`*`organization _name`*`, dc=`*`company`*`, dc=com bindpw=`*`password`*
Log Detail (`logdetail=`)	None	*None* | *High* | *Medium* | *Low* |*Trace* 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**: `set /SP/clients/ldapssl/ logdetail=`*`none`*`|`*`high`*`|`*`medium`*`|`*`low`*`|`*`trace`*
Save		**Web interface** – To apply changes made to properties within the LDAP/SSL Settings page, you must click Save.

Table 3-20 Uploading or Removing an LDAP/SSL Certificate File

User Interface Configurable Target:

- **CLI: `/SP/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	*Certificate Present* |*Certificate Not Present* The Certificate File Status property indicates whether an LDAP/SSL certificate has been uploaded to Oracle ILOM. **CLI Certificate Status Syntax**: `show /SP/clients/ldapssl/cert`
File Transfer Method	Browser (web interface only)	*Browser*|*TFTP*|*FTP*|*SCP*|*Paste* For a detailed description of each file transfer method, see File Transfer Methods .
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/clients/ldapssl/cert clear_action=true`
		-or-
		`reset /SP/clients/ldapssl/cert`
		When prompted, type `y` to continue the action or `n` to cancel the action.

Table 3-21 Optionally Configuring LDAP/SSL Groups

User Interface Configurable Target:

- **CLI: `/SP/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/clients/ldapssl/admingroups/`*`n`*` name=`*`string`*
	`set /SP/clients/ldapssl/admingroups/`*`n`*` name=`*`[string]`*
	Example Syntax:
	`set /SP/clients/ldapssl/admingroups/1/ name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com`
	`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.
	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.
	`set /SP/clients/ldapssl/operatorgroups/`*`n`*` name=`*`string`*
	Example Syntax:
	`set /SP/clients/ldapssl/operatorgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com`
	`Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com''`

Table 3-21 (Cont.) Optionally Configuring LDAP/SSL Groups

User Interface Configurable Target:

- **CLI: `/SP/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
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:** `set /SP/clients/ldapssl/hostgroups/`*`n`*`/ name=`*`string`* `hosts=`*`string`*` roles=`*`string`* 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.

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 Enabling LDAP/SSL Authentication .
	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:
	`set /SP/clients/ldapssl/customgroups/`*`n`*` name=`*`string`*
	`roles=`*`administrator`*`|`*`operator`*`|`*`a`*`|`*`u`*`|`*`c`*`|`*`r`*`|`*`o`*`|`*`s`*
	Example Syntax:
	`set /SP/clients/ldapssl/customgroups/1`
	`name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com`
	`roles=au`
	`Set 'name' to`
	`'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com''`
	`roles' to 'au'`
	Related Information:
	• Assignable Oracle ILOM User Roles

Save	**Web interface** – To apply changes made to properties in the Admin, Operator, or Custom Group dialogs, you must click Save.

Table 3-22 Configuring LDAP/SSL User Domains

User Interface Configurable Target:

- **CLI: `/SP/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.
	• 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 /SP/clients/ldapssl/userdomains/`*`n`* `domain=`*`string`*
	Example 1: `domain=CN=<USERNAME>`
	`set /SP/clients/ldapssl/userdomains/1 domain=CN=<USERNAME>,OU=Groups,DC=sales,DC-oracle,DC=com`
	Set 'domain' to 'CN=<USERNAME>,OU=Groups,DC=sales,DC=oracle,DC=com'
	Example 2: domain=CN=spSuperAdmin
	`set /SP/clients/ldapssl/userdomains/1 domain=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com`
	`Set 'domain' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com'`
	Example 3: Searchbase syntax using `<BASE:`*`string`*`>`
	`set /SP/clients/ldapssl/userdomains/1 domain=uid=<USERNAME>,ou=people,dc=oracle,dc=com<BASE:ou=doc,dc=oracle,dc=com>`

Save	**Web interface** – To apply changes made to properties in the LDAP/SSL User Domain dialog, you must click Save.

Table 3-23 Optionally Configuring LDAP/SSL Alternate Servers

User Interface Configurable Target:

- **CLI: `/SP/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
(*/1|2|3|4|5*)
	Oracle ILOM enables you to configure up to five LDAP/SSL alternate servers.
	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:
	`set /SP/clients/ldapssl/alternateservers/n address=sting port=string`
	CLI Alternate Server s Certificate Syntax:
	`show /SPclients/ldapssl/alternateservers/n/cert`
	`load_uri=file_transfer_method://host_address/file_path/filename`
	`set /SP/clients/ldapssl/alternateservers/n/cert clear_action=true`

Save	**Web interface** – To apply changes made to properties in the LDAP/SSL Alternate Servers dialog, you must click Save.

Table 3-24 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:

- Enabling LDAP/SSL Authentication
- Managing Oracle ILOM Log Entries
- Setting ILOM Clock Properties

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:

- Requirements for Enabling Oracle ILOM as an LDAP Client Requirements for Enabling Oracle ILOM as an LDAP Client
- Enabling Oracle ILOM to Use LDAP Authentication Enabling Oracle ILOM to Use LDAP Authentication

Table 3-25 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 (RC2307) (http://www.ietf.org/rfc/rfc2307.txt)

Table 3-26 Enabling Oracle ILOM to Use LDAP Authentication

User Interface Configurable Target:

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

Property	Default Value	Description
State (`state=`)	Disabled	*Disabled |Enabled* 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 /SP/clients/ldap/ state=`*`disabled`*`|`*`enabled`*

Table 3-26 (Cont.) Enabling Oracle ILOM to Use LDAP Authentication

User Interface Configurable Target:

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

Property	Default Value	Description
Roles (`defaultrole=`)	Operator	*Administrator |Operator |Advanced* 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 /SP/clients/ldap/ defaultrole=administrator|operator|a|u|c|r|o|s` **Related Information:** • Privileges Granted by a User Profile • Privileges Granted by Individual User Roles
Address (`address=`)	0.0.0.0	*IP address| DNS host name* (LDAP Server) 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 /SP/clients/ldap/ address=ldap_server ip_address|ldap_server_dns_host_name` **Related Information:** • DNS Configuration Properties
Port (`port=`)	389	*389* | *User-specified TCP port* TCP port 389 is used by Oracle ILOM to communicate with the OpenLDAP server. If necessary, configure Oracle ILOM to use another port by modifying the default Port number: 389 **CLI Port Syntax**: `set /SP/clients/ldap/ port=number`

Table 3-26 (Cont.) Enabling Oracle ILOM to Use LDAP Authentication

User Interface Configurable Target:

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

Property	Default Value	Description
Searchbase (`searchbase=`)		`ou=` *organization_unit* |`dn=`*domain_name*|`dc=`*domain*| The Searchbase is the location in the LDAP tree where Oracle ILOM searches to validates 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: ou=IT, dc=mycompany, dc=.com **CLI Searchbase Syntax**: `set /SP/clients/ldap/ searchbase= ou=`*`organization_name`*`, dn=` *domain_name*, `dc=`*domain*
Bind DN (`binddn=`)		`ou=`*organization_unit* |`dn=`*domain_name*|`dc=`*domain*|`cn=`*common_name* 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/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/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 3-27 Enabling Oracle ILOM to Use RADIUS Client Server Authentication

User Interface Configurable Target:

- **CLI: `/SP/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.**

<table>
<tr><th>Property</th><th>Default Value</th><th>Description</th></tr>
<tr><td>State
(<code>state=</code>)</td><td>Disabled</td><td><i>Disabled |Enabled</i>
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.
<b>CLI RADIUS State Syntax</b>:
<code>set /SP/clients/radius/ state=<i>disabled</i>|<i>enabled</i></code></td></tr>
<tr><td>Roles
(<code>defaultrole=</code>)</td><td>Operator</td><td><i>Administrator |Operator |Advanced</i>
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 (<i>a</i>|<i>u</i>|<i>c</i>|<i>r</i>|o|<i>s)</i>.
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.
<b>CLI Roles Syntax</b>:
<code>set /SP/clients/radius/ defaultrole=<i>administrator</i>|<i>operator</i>|<i>a</i>|<i>u</i>|<i>c</i>|<i>r</i>|<i>o</i>|<i>s</i></code>
<b>Related Information:</b>
• Privileges Granted by a User Profile
• Privileges Granted by Individual User Roles</td></tr>
<tr><td>Address
(<code>address=</code>)</td><td>0.0.0.0</td><td><i>IP address</i>| <i>DNS host name</i> (LDAP Server)
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.
<b>CLI Address Syntax</b>:
<code>set /SP/clients/radius/ address=<i>radius_server ip_address</i>|<i>ldap_server_dns_host_name</i></code>
<b>Related Information:</b>
• DNS Configuration Properties</td></tr>
<tr><td>Port
(<code>port=</code>)</td><td>1812</td><td><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
<b>CLI Port Syntax</b>:
<code>set /SP/clients/radius/ port=<i>number</i></code></td></tr>
</table>

Table 3-27 (Cont.) Enabling Oracle ILOM to Use RADIUS Client Server Authentication

User Interface Configurable Target:

- **CLI: `/SP/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
Shared Secret (`secret=`)		Populate the Shared Secret property with the known RADIUS client server shared password. The RADUS client server model uses the shared password to recognize each other, and to protect sensitive user credential data. **CLI Shared Secret Syntax**: `set /SP/clients/radius/ secret=`*`password`*
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**: `set /SP/clients/radius/alternateservers/`*`1|2|3|4|5`*`/ address=`*`radius_server ip_address| ldap_server_dns_host_name`* `port=`*`number`* `secret=`*`password`* **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.

4

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
Refer to this section for management access requirements and configuration properties.	• Modifying Default Management Access Configuration Properties
Refer to this section for connectivity requirements and configuration properties.	• Modifying Default Connectivity Configuration Properties
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 • Setting ILOM Clock Properties
Refer to this section for guidelines for resolving management access and network connectivity issues.	• Suggested Resolutions for Network Connectivity Issues

Related Information

- Oracle ILOM Deployment Practices for Increasing Security
- Logging In to Oracle ILOM

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
- Network Connectivity Deployment Options
- Operating Oracle ILOM in FIPS Compliance Mode
- Use of Web Server Certificates and SSH Server-Side Keys
- Default Timeout for CLI and Web Sessions
- Management of Banner Messages at Log-In
- Input Format for IPv4 and IPv6 Addresses
- Serial Management Port Owner
- Default Network Ports Used by Oracle ILOM
- Legacy Oracle Servers Not Supporting IPv6

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 4-1 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 • 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. 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 • Use of Web Server Certificates and SSH Server-Side Keys • Web Server Configuration Properties
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. Oracle ILOM automatically generates the server-side SSH keys on the first boot of a factory default system. **Related Information:** • SSH Server Configuration Properties • Operating Oracle ILOM in FIPS Compliance Mode • Use of Web Server Certificates and SSH Server-Side Keys

Table 4-1 (Cont.) Management Access Deployment Options and Default Settings

Management Access	Management Service	Defaults	Description
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 SNMP v3 enabled for monitoring. **Related Information:** • SNMP Configuration Properties • Operating Oracle ILOM in FIPS Compliance Mode • Configuring SNMP Settings in Oracle ILOM • Alert Notification Configuration Properties
IPMItoolclient	• IPMI	• IPMI v2 over port 623, enabled • IPMI Service state enabled (default) • IPMI v2 Sessions disabled (default)	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. **Related Information:** • IPMI Service Configuration Properties • Operating Oracle ILOM in FIPS Compliance Mode • Assignable Oracle ILOM User Roles • Server Management Using IPMI • Alert Notification Configuration Properties

Network Connectivity Deployment Options

The connectivity options in Oracle ILOM arrive preconfigured so Oracle ILOM can learn the physical server SP 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 4-2 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, Oracle ILOM will attempt to learn the physical address for the SP 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:** • Network Connectivity Standard Configuration Properties • Sideband Network Management Connection • Dedicated Network Management Connection (Default)
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. 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:** • DNS Configuration Properties • Example Setup of Dynamic DNS
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:** • Serial Port Configuration Properties • Serial Management Port Owner • Dedicated Network Management Connection (Default)

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
- FIPS Compliance Mode Effect on ILOM Configuration Properties
- Unsupported Features When FIPS Mode Is Enabled

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 and Unsupported Features When FIPS Mode Is Enabled.
- 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`
2. Configure the FIPS State property as described in Federal Information Processing Standards (FIBS 140-2) Configuration Properties.

   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 Federal Information Processing Standards (FIBS 140-2) Configuration Properties.
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`

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 4-3 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.

Table 4-3 (Cont.) Guidelines for Deploying a Server or Updating a Server with FIPS Mode

Guideline	Description
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 . 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"). • 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. 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 . 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 . **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
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. **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

Oracle ILOM arrives with the SSH Server State property enabled. Administrators can choose to use these defaults settings as is or modify them. For futher details about configuring these properties, see SSH Server Configuration Properties.

Use of Web Server Certificates and SSH Server-Side Keys

Oracle ILOM arrives preconfigured with SSL 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. In addition to the SSL certificates and SSH server side key support, Oracle ILOM, as of firmware version 5.0, enables administrators to store up to five server certificates to validate outgoing HTTPS connections.

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. The generated SSH server-side keys can be regenerated as needed, and the outgoing HTTPS server certificates can be uploaded as required to help prevent man-in-the-middle attacks. For further configuration information, see the following:

- SSL Certificate and Private Key Configuration Properties for HTTPS Web Server.
- SSH Server Configuration Properties
- Server Certificate Configuration Properties for Outgoing HTTPS Connections

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 720 minutes (12 hours). 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 CLI Session Timeout and Custom Prompt Configuration Properties. For web session timeout configuration properties, see Web Server Configuration Properties.

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
- Delete a Banner Message
- Control Message Acceptance Behavior for Login Message

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/preferences/banner/[*connect* | *login*]

     where:

     - *SP* = Server SP management
     - *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.
   - 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.
       * *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/preferences/banner/[` *connect* | *login*] `message=""`

    where:
    - *SP* = Server SP management
    - *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:
      1. 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.
      2. Click Save.
    - To continue without acceptance:
      1. 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.
      2. Click Save.
  - CLI: Type the following command string to set the applicable message acceptance behavior:
    ```
    set /SP/preferences/banner/login message_acceptance= [enabled
    | disabled]
    ```

    where:
    - *SP* = Server SP management

- *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: *n.n .n.n* **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 Serial Port Configuration Properties .

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 4-4 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

Table 4-4 (Cont.) Oracle ILOM Default Network Ports

Port	Protocol	Application
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol (outgoing)
80	HTTP Redirection 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 ConsoleILOM 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

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:

- Web Server Configuration Properties
- SSL Certificate and Private Key Configuration Properties for HTTPS Web Server
- SSH Server Configuration Properties
- Server Certificate Configuration Properties for Outgoing HTTPS Connections
- SNMP Configuration Properties
- IPMI Service Configuration Properties
- CLI Session Timeout and Custom Prompt Configuration Properties
- Federal Information Processing Standards (FIBS 140-2) Configuration Properties
- Servicetag Service Configuration Properties

Table 4-5 Web Server Configuration Properties

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
Service State `(serverstate=)`	Enabled, HTTP Redirection Enabled	Enabled, HTTP Redirection Enabled (default) | Enabled, HTTP Redirection Disabled | Disabled • Enabled, HTTP Redirection Enabled (default) — Set this setting to: 1) enable HTTPS web server connections, and 2) automatically redirect HTTP requests to HTTPS • Enabled, HTTP Redirection Disabled — Set this setting to: 1) enable HTTPS web server connections, and 2) disable HTTP redirection requests to HTTPS. • Disabled — Set this setting to disable the Service State for the Oracle ILOM web server. When disabled, all HTTPS web server connections are disabled, as well as all HTTP redirection requests to HTTPS. **Requirement**: An SSL certificate is required for enabled HTTPS connections. You can choose to use the Oracle ILOM provided SSL certificate or upload a custom SSL certificate and a matching private key using the Management Access > SSL Certificate tab. **CLI Syntax for Secure Redirect and Service State**: `set SP/services/web secureredirect=`*`disabled`*`|`*`enabled`*`servicestate=`*`disabled`*`|`*`enabled`*
HTTP Port `(http_port=)`	80	*80 |User_defined* When the Service State property is set to "Enabled, HTTP Redirection Enabled", Oracle ILOM communicates, by default, using HTTP over TCP port 80. If necessary, the default HTTP port number (80) can be modified. **CLI Syntax for HTTP Port**: `set SP/services/web http_port=<`*`n`*`>`
HTTPS Port `(https_port=)`	443	*443 |User_defined* When the Service Sate property is set to either "Enabled, HTTP Redirection Enabled" or "Enabled, HTTP Redirection Disabled", Oracle ILOM communicates, by default, using HTTPS over TCP port 443. If necessary, the default HTTPS port number (443) can be modified. **Requirement**: The Oracle ILOM web server HTTP and HTTPS ports must be different. **CLI Syntax for HTTPS Port**: `set SP/services/web https_port=<`*`n`*`>`

Table 4-5 (Cont.) Web Server Configuration Properties

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
TLS v1.2, (`tlsv1_2 =`)	TLS v1.2 Enabled	*Enabled |Disabled* Transport Layer Security (TLS) protocols provide communication security over the Internet. Enabled — When set to Enabled, the TLSv1.2 communication protocol in Oracle ILOM is enabled. Disabled — .When set to Disabled, the TLSv1.2 communication protocol in Oracle ILOM is disabled. This configuration action prevents the Oracle ILOM SSL interfaces (Oracle ILOM web, IPMItool, and so on) from negotiating connections. **CLI Syntax for TLSv1.2** `set /SP/services/web tlsv1_2= enabled|disabled`
Session Timeout (`sessiontimeout=`)	15 seconds	*15 seconds |User_defined* The Session Timeout property controls the amount of time before Oracle ILOM terminates an inactive web client session. The default Session Timeout is 15 seconds. The maximum Session Timeout is 12 hours (720 minutes). **Note.** The session timeout property in the Oracle ILOM web interface can be set in any combination of hours or minutes. The Oracle ILOM CLI session timeout property must be specified in minutes. **CLI Syntax for Session Timeout**: `set /SP/services/web sessiontimeout=<n>`
Session Duration (sessionduration=)	24 Hours (14400 Minutes)	24 Hours default | *User_defined* The Session Duration property controls the amount of time that the client browser is allowed to keep the session cookie. The default Session Duration is 24 hours. The maximum Session Duration is 240 hours (14400 minutes). **Note:** The session duration property in the Oracle ILOM web interface can be set in any combination of hours or minutes. The Oracle ILOM CLI session timeout property must be specified in minutes. **CLI Syntax for Session Duration**: `set /SP/services/web sessionduration=<n>` **Note.** Setting the Session Duration to zero (0) in the Oracle ILOM CLI disables the Session Duration feature.
Allowed Services (`allowedservices=`)		Browser and REST (default) | Browser | REST The Allowed Services property controls which web services are allowed to communicate with Oracle ILOM. The Browser and REST services are enabled by default. **CLI Syntax for Allowed Services**: `set /SP/services/web allowedservices=<browser|rest|browser,rest|rest,browser>`
Save		**Web interface** – To apply changes made to properties within the Web Server Settings page, you must click Save.

Table 4-6 SSL Certificate and Private Key Configuration Properties for HTTPS Web Server

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

- **CLI: `/SP/services/web/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)	*Default_Certificate* |*Custom_Certificate* 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 The default self-signed SSL certificate ensures that all communication between a web browser client and the Oracle ILOM SP is fully encrypted. **CLI Syntax to Show Certificate Status**: `show /SP/web/ssl`
Default SSL Certificate Key Size (/default_cert `generate_new_cert_keysize =`)	3072	2048 | *3072 (default)* |*4096* **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/web/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.

Table 4-6 (Cont.) SSL Certificate and Private Key Configuration Properties for HTTPS Web Server

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

- **CLI: `/SP/services/web/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
Create Default SSL Certificate (default_cert `generate_new_cert_action` =)	N/A	Each Oracle ILOM SP 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 **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 (`show /SP/services/web/ssl/default_cert fingerprint`). **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/web/ssl/default_cert generate_new_cert_action =true` 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.

Table 4-6 (Cont.) SSL Certificate and Private Key Configuration Properties for HTTPS Web Server

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

- **CLI: `/SP/services/web/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
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_file name`* Where *file_transfer_method* can include: *Browser*|*TFTP*|*FTP*|*SCP*|HTTP | HTTPS|*Paste* For a detailed description of each file transfer method (excluding Paste), see Supported File Transfer Methods 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. **Note:** Oracle ILOMgenerates a warning message when a custom certificate and private key are not properly configured. For further details, see Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate **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 Uploading an SSL Certificate for ASR Client Configurations .
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/services/web/ssl/custom_certificate clear_action=true` When prompted, type `y` to delete or `n` to cancel action.

Table 4-6 (Cont.) SSL Certificate and Private Key Configuration Properties for HTTPS Web Server

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

- **CLI: `/SP/services/web/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
Custom Private Key (/ `custom_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. **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**: `load_uri=`*`file_transfer_method`*`://`*`host_address`*`/`*`file_path`*`/`*`custom_key_file name`* Where *file_transfer_method* can include: *Browser*|*TFTP*|*FTP*|*SCP*|HTTP | HTTPS|*Paste*For a detailed description of each file transfer method (excluding Paste), see Supported File Transfer Methods. 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.
Custom Private Key Remove (`/custom_key clear_action =true`)		**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**: `set /SP/services/web/ssl/custom_key clear_action=true` When prompted, type `y` to delete or `n` to cancel the action.

Table 4-7 SSH Server Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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	*Enabled |Disabled* 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 using a command-line interface. When the SSH Server State property is disabled or restarted, all CLI SP 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 *not* require you to restart the SSH server. **CLI Syntax for SSH Server State**: `set /SP/services/ssh state=`*`enabled|disabled`*
Restart Button (`restart_sshd_action=`)		*True|False* Restarting the SSH server will automatically: (1) terminate all connected SP CLI sessions, as well as (2) activate newly pending server-side key(s). **CLI Syntax for Restart:** `set /SP/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/services/ssh generate_new_key_type=rsa generate_new_key_action=true`

Table 4-8 Server Certificate Configuration Properties for Outgoing HTTPS Connections

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

- **CLI: `/SP/preferences/servercerts`**
- **Web: ILOM Administration > Management Access > Server Certificate**
- **User Role: admin(a) (required for all property modifications)**
- **Requirement: The SSL server certificate files must be in PEM (Privacy Enhanced Mail) format, and they must not be encrypted with a passphrase. When uploading an SSL server certificate, the SSL certificate and key set must match.**

Property	Default Value	Description
Strict Certificate Mode (`strictcertmode=`)	Disabled	*Enabled* | *Disabled* (default) The Strict Certificate Mode property controls whether Oracle ILOM checks the validity of the SSL server certificate when uploading the SSL server certificate to the server SP. • When disabled (default), Oracle ILOM is prevented from checking the validity of the SSL certificates. • When enabled, Oracle ILOM checks the validity of the SSL server certificate when operations such as the following are performed: 1) Backing up or restoring of BIOS configuration, 2) Downloading of the firmware image, 3) Updating the firmware image, 4) Downloading of SSL certificates (SSL certificates are only subject to certificate verification when Strict Certificate Mode is enabled), 5) Downloading of SSH keys and 6) Backing up or restoring Oracle ILOM configuration. **Note:** In cases where Oracle ILOM is not able to validate the authenticity of the SSL server certificate, an error message appears indicating the reason why the operation failed. **Web interface –** Select the Strict Certificate Mode check box to enable this feature or clear the check box to disable this feature. **CLI Syntax to Remove Certificate**: `set /SP/preferences/servercerts strictcertmode=` *`enabled`* `|` *`disabled`*

Table 4-8 (Cont.) Server Certificate Configuration Properties for Outgoing HTTPS Connections

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

- **CLI: /SP/preferences/servercerts**
- **Web: ILOM Administration > Management Access > Server Certificate**
- **User Role: admin(a) (required for all property modifications)**
- **Requirement: The SSL server certificate files must be in PEM (Privacy Enhanced Mail) format, and they must not be encrypted with a passphrase. When uploading an SSL server certificate, the SSL certificate and key set must match.**

Property	Default Value	Description

Add SSL Certificates
`(/load_uri=)`
- or -
Delete SSL Certificates
`(/# clear_action =true)`
		System administrators can store up to five trusted SSL server certificates. Oracle ILOM uses these certificates to prevent man-in-the-middle-attacks when uploading and downloading data to and from the Oracle ILOM SP using HTTPS.
		Web interface –To add or remove a certificate, click the More Details ... link at the top of the Server Certificates page for instructions.
		CLI Syntax to Load SSL Server Certificate
		`load_uri=`*`file_transfer_method`*`://`*`host_address/ file_path/PEM file name`*
		Where *file_transfer_method* can include: *Browser*|*TFTP*|*FTP*|*SCP*|HTTP | HTTPS|*Paste*For a detailed description of each file transfer method (excluding Paste), see Supported File Transfer Methods.
		CLI Syntax to Delete SSL Server Certificate
		`set /SP/preferences/servercerts/<`*`1-5`*`> clear_action=true`
		Are you sure you want to clear /SP/preferences/servercerts/# (y/n)?
		Type: `y`
		For additional information about using SSL Certificates in Oracle ILOM, see Improve Security by Using a Trusted SSL Certificate and Private Key.

Save		**Web interface –** Click Save to save the changes made to the Server Certificate page.

Table 4-9 SNMP Configuration Properties

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

- **CLI: `/SP/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 SNMP v3 services .**

> **Note:**
>
> **SNMP set operations and writeable SNMP MIBs are no longer supported in Oracle ILOM as of firmware version 4.0.x.**

Property	Default Value	Description
State (`state=`)	Enabled	*Enabled* |*Disabled* 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**: `set /SP/services/snmp state=`*`enabled`*`|`*`disabled`*
Port (`port=`)	161	*161* | *User_specified.* Oracle ILOM, by default, uses UDP port 161 to transmit SNMP communication between an Oracle ILOM SP and the network. If necessary, the default port property number can be changed. **CLI Syntax for SNMP Port**: `set /SP/services/snmp port=`*`n`*
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.
Protocols (v3)	v3 Enabled	Enabled (default) | Disabled SNMP v3 is enabled by default, but requires creating one or more SNMP users prior to use. There are no preconfigured SNMPv3 users. SNMPv3 uses encryption to provide a secure channel and the use of SNMP v3 user names and passwords that are stored securely on the SNMP management station. SNMP v3 is configurable property for monitoring the health of a system. SNMP v2c is a non-configurable property that is only supported for trap alert notifications. **CLI Syntax to Modify Default Protocol:** `set /SP/services/snmp `*`v3=enabled`*`|`*`disabled`*
Save		**Web interface** – To apply changes made to properties within the SNMP Management page, you must click Save.

Table 4-9 (Cont.) SNMP Configuration Properties

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

- **CLI: `/SP/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 SNMP v3 services .**

> **Note:**
>
> **SNMP set operations and writeable SNMP MIBs are no longer supported in Oracle ILOM as of firmware version 4.0.x.**

Property	Default Value	Description

SNMP Users
(`/users`)
		Username | *Authentication Password* | *Permission*| *Authentication Protocol* | *Privacy Protocol*
		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 *not* contain spaces.
		• 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:
		`create /SP/services/snmp/users/[new_username] authenticationprotocol=[MD5|SHA] authenticationpassword=[changeme] permission=[ro|rw] privacyprotocol=[AES|DES|none] privacypassword=[user_password]`
		`show /SP/services/snmp/users`
		`delete /SP/services/snmp/username`
		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.

Table 4-10 IPMI Service Configuration Properties

User Interface Configurable Target:

- **CLI: `/SP/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	*Enabled (default)*|*Disabled* As of Oracle ILOM firmware version 3.2.8, the State property for IPMI TLS service is enabled by default. When the IPMI State property is enabled, Oracle ILOM permits remote IPMItool clients to securely connect to the Oracle ILOM SP using a command-line interface. When the IPMI State property is disabled, all IPMItool clients connected to the SP through the Oracle ILOM CLI are automatically terminated. **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 /SP/services/ipmi state=`*`enabled`*|*`disabled`*
v2.0 Sessions (`v2_0_sessions=`)	Disabled	*Disabled (default)* | *Enabled* The v2.0 Sessions check box controls whether Oracle ILOM permits IPMI v2.0 connections. **Web interface:** Select the v2.0 Sessions check box to permit IPMI v2.0 connections with Oracle ILOM. When IPMI 2.0 sessions are enabled, users of IPMItool specify the -I lanplus option. **Note:** IPMI v2.0 Sessions use standard IPMI protocol and work with any IPMI client. - **or** - Clear the v2.0 Sessions check box to prevent (block) IPMI v2.0 sessions with Oracle ILOM. **Note:** Changes to the IPMI State in the web interface do not take affect in Oracle ILOM until you click Save. **CLI Syntax for v2.0 Sessions**: `set /SP/services/ipmi v2_0_sessions=`*`enabled`*|*`disabled`*

Table 4-10 (Cont.) IPMI Service Configuration Properties

User Interface Configurable Target:

- **CLI: `/SP/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	*Enabled (default) |Disabled* 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 To access the IPMI TLS interface, IPMItool users can either specify the `–I orcltls` option or not specify an option and IPMItool will automatically detect the most secure interface available. For more information about using the TLS service and interface, see the following information: • IPMI TLS Service and Interface. • Configure IPMI Management Access for Increased Security.

Table 4-11 CLI Session Timeout and Custom Prompt Configuration Properties

User Interface Configurable Target:

- **CLI: `/SP/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=`)	Enabled (12 hours)	*Enabled, minutes=n* | *Disabled* The CLI Session Timeout property determines how many minutes until an inactive CLI session is automatically logged out. As of Oracle ILOM firmware version 5.0.1, the CLI session timeout property is set by default to 12 hours (720 minutes). When necessary, you can modify the default CLI session timeout value by entering a value (in minutes) from 1 to 1440. **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 /SP/cli timeout=`*`enabled`*`|`*`disabled`* `minutes=` *value*
Custom Prompt (`prompt=`)	None (disabled)	*None (default)* | *["Literal Text"]* | "<HOSTNAME>" | "<IPADDRESS>" To help identify a standalone system or a system within a rack or chassis, Administrators can customize the standard CLI prompt (->) by prepending either literal text, replacement tokens ("<HOSTNAME>" "<IPADDRESS>"), 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 *More details...* link on the Management Access > CLI page. **CLI Syntax for Custom CLI Prompt**: Examples: • `set /SP/cli prompt=`*"Literal_Text"* • `set /SP/cli prompt=` "*<HOSTNAME>*" • `set /SP /cli prompt="`*`<IPADDRESS>`*`"` • `set /SP/cli prompt=` *["Literal_Text"]* `"<HOSTNAME>"` • `set /SP/cli prompt=` *["Literal_Text"]* `"<HOSTNAME>" "<IPADDRESS>"`

Table 4-12 Federal Information Processing Standards (FIBS 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 *Disabled* 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 *does not* appear in the masthead area of the Oracle ILOM window. • Enabled — The Status for *Enabled* 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 *Disabled; enabled at next boot* 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 *does not* appear in the masthead area of the Oracle ILOM window. • Enabled; disabled at next boot — The *Status for Enabled; disabled at next boot* 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 • Unsupported Features When FIPS Mode Is Enabled

Table 4-12 (Cont.) Federal Information Processing Standards (FIBS 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
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 • FIPS Compliance Mode Effect on ILOM Configuration Properties

Table 4-13 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	|*Enabled* (default) |*Disabled* 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. **Note:** 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=` *`disabled`*`|`*`enabled`*

Table 4-13 (Cont.) 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
`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:

- Network Connectivity Standard Configuration Properties 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.

- Network Connectivity Enhanced Configuration Properties 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.

- DNS Configuration Properties
- Serial Port Configuration Properties

> **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 4-14 Network Connectivity Standard Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
State (`state=`)	Enabled	*Enabled |Disabled* 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 /SP/network state=`*`enabled|disabled`*

MAC Address
Out of Band MAC Address
Sideband MAC Address
	Read-only	`macaddress=`| `outofbandaddress=` | `sidebandmacaddress=`
		The media access control (MAC) addresses for the server SP are set at the factory.
		The SP MAC Address properties are non-configurable read-only properties.
		CLI Syntax to Show MAC Address Properties:
		`show /SP/network`

Table 4-14 (Cont.) Network Connectivity Standard Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
Management Port (`managementport=`)	MGMT	*MGMT |NETn* 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 (NET*n*) 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 (NET*n*). **CLI Syntax for SP Management Port:** `set /SP/network pendingmanagementport=`*`MGMT`*`|`*`NETn`* `set /SP/network commitpending=true` **Related Information**: • Sideband Network Management Connection • Dedicated Network Management Connection (Default)

VLAN Tag
`(pendingvlan_id=)`
	(none)	*Integer between 1 and 4079*
		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:
		`set /SP/network pendingvlan_id=[`*`1-4079`*`|""]`
		`commitpending=true`

Table 4-14 (Cont.) Network Connectivity Standard Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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 IP Discovery Mode (`ipdiscovery=`)	DHCP	*DHCP |Static* 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. 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. **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**: `set /SP/network pendingipdiscovery=`*`dhcp`*`|`*`static`* `set /SP/network commitpending=true` **Related Information**: • DNS Configuration Properties
IPv4 DHCP Client ID (`dhcp_clientid=`)	None	*None|SysID* 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 `system_identifier` property under the `/SP` target. **CLI Syntax for IPv4 DHCP Client ID**: `show /SP/network dhcp_clientid=`*`none`*`|`*`sysid`* **Related Information**: • Assigning System Identification Information

Table 4-14 (Cont.) Network Connectivity Standard Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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 Network Address Netmask Address Gateway Address	Static IP Discovery Mode, Disabled	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**: `set /SP/network pendingipaddress=`*`value`* `pendingipnetmask=`*`value`* `pendingipgateway=`*`value`* `set /SP/network commitpending=true` **Related Information**: • Input Format for IPv4 and IPv6 Addresses
IPv6 State (`/ipv6/ state=`)	Enabled	*Enabled* |*Disabled* 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. **CLI Syntax for IPv6 State**: `set /SP/network/ipv6 state=`*`enabled`*`|`*`disabled`*

Table 4-14 (Cont.) Network Connectivity Standard Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
IPv6 Autoconfig (`/ipv6 autoconfig=`)	Stateless	disabled|stateless 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:** • 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 /SP/network/ipv6 autoconfig=`*`stateless`*`|` *`disabled`*

Table 4-14 (Cont.) Network Connectivity Standard Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
DHCPv6 Autoconfig (`/ipv6 autoconfig=`)	(none)	*DHCPv6_Stateless |DHCP_Stateful* The DHCPv6 Autoconfig property is disabled in Oracle ILOM by default. When this property is disabled, Oracle ILOM is prevented from learning the SP network address 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 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 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 dhcpv6_server_duid property. **CLI Syntax for DHCPv6 Autoconfig**: `set /SP/network/ipv6 autoconfig=`*`dhcpv6_stateless`*`|`*`dhcpv6_stateful`*
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 from another IPv6-enabled node on the same network. Oracle ILOM applies the following principles to build the Link-Local Address for the SP: • Oracle ILOM uses the SP 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 is unique. **CLI Syntax for Link-Local Address:** `show /SP/network/ipv6`

Table 4-14 (Cont.) Network Connectivity Standard Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
IPv6 Static IP Address (`/ipv6 static_ipaddress=`)	None	When the IPv6 state is enabled, network administrators can optionally assign a static IPv6 address to the SP. **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: *IPv6_address*/ *subnet_mask_length_in_bits*. The gateway address, is automatically configured. **Example**: fec0:a:8:b7:214:4fff:feca:5f7e/64 **CLI Syntax for Static IPv6 Address**: `set /SP/network/ipv6 pending_static_ipaddress=`*`ipaddress`*`/`*`subnetmask`* `set /SP/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/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. **Special Considerations**: • Oracle ILOM stores up 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/network/ipv6`

Table 4-14 (Cont.) Network Connectivity Standard Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
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. 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 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. **CLI Syntax for IPv4 Commit Pending Modification**: `set /SP/network state=`*`enabled`*`|`*`disabled`* `pendingipdiscovery=`*`static`*`|`*`dhcp`* `pendingipaddress=`*`value`* `pendingipgateway=`*`value`* `pendingipnetmask=`*`value`* `set /SP/network commitpending=true` **CLI Syntax for IPv6 Commit Pending Modifications:** `set /SP/network/ipv6 state=`*`enabled`*`|`*`disabled`* `pending_static_ipaddress=`*`ipv6_address`*`/`*`subnet_mask_length_in_bits`* `set /SP/network commitpending=true` **Related Information**: • Test IPv4 and IPv6 Connectivity

Table 4-15 Network Connectivity Enhanced Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
Out of Band MAC Address
Sideband MAC Address
	Read-only	`macaddress=`| `outofbandaddress=` | `sidebandmacaddress=`
		The media access control (MAC) addresses for the server SP are set at the factory.
		The SP MAC Address properties are non-configurable read-only properties.
		CLI Syntax to Show MAC Address Properties:
		`show /SP/network`

Management Port (`managementport=`)	MGMT	*MGMT* |*NETn* 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 (NET*n*) 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 (NET*n*). **CLI Syntax for SP Management Port:** `set /SP/network pendingmanagementport=`*`MGMT`*`|`*`NETn`* `set /SP/network commitpending=true` **Related Information**: • Sideband Network Management Connection • Dedicated Network Management Connection (Default)

Table 4-15 (Cont.) Network Connectivity Enhanced Configuration Properties

<table>
<tr><td colspan="3"><b>User Interface Configurable Target and User Role:</b><ul><li><b>CLI: <code>/SP/network</code></b></li><li><b>Web: ILOM Administration > Connectivity > Network > Network Settings</b></li><li><b>User Role: admin (a) (required for all property modifications)</b></li></ul><b>Requirements:</b><ul><li><b>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.</b></li><li><b>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.</b></li></ul></td></tr>
<tr><th>Property</th><th>Default Value</th><th>Description</th></tr>
<tr><td>VLAN Tag
<code>(pendingvlan_id=)</code></td><td>(none)</td><td><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.
<b>CLI Syntax for VLAN Tag:</b>
<code>set /SP/network pendingvlan_id=[<i>1-4079</i>|””] commitpending=true</code></td></tr>
<tr><td>IPv4 State
<code>(state=)</code></td><td>Enabled</td><td><i>Enabled |Disabled</i>
The IPv4 network State property is enabled by default.
<b>Web Property Descriptions for IPv4 State:</b><ul><li>Enabled (default) — When the Enabled check box for IPv4 State is selected, the Ethernet connection to Oracle ILOM is enabled for IPv4.</li><li>Disabled — When the Enabled check box for IPv4 State is cleared, the Ethernet connection to Oracle ILOM is disabled for IPv4.</li></ul><b>CLI Syntax and Property Descriptions for IPv4 State</b>:
<code>set /SP/network state=<i>enabled</i>|<i>ipv4-only</i>|<i>ipv6-only</i>|<i>disabled</i></code>
<b>CLI IPv4 Property Descriptions</b><ul><li><code>enabled</code> (default) — Set to <code>enabled</code> 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 <code>enabled</code>.</li><li><code>ipv4-only</code> — When set to <code>ipv4-only</code>, the Ethernet connection to Oracle ILOM is enabled for IPv4 only.</li><li><code>ipv6-only</code> — When set to <code>ipv6-only</code>, the Ethernet connection to Oracle ILOM is enabled for IPv6 only.</li><li><code>disabled</code> — Set to <code>disabled</code> to prevent both an IPv4 and an IPv6 Ethernet connection to Oracle ILOM.</li></ul></td></tr>
</table>

Table 4-15 (Cont.) Network Connectivity Enhanced Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
IPv4 IP Discovery Mode (`ipdiscovery=`)	DHCP	*DHCP |Static* 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. 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. **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. **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 /SP/network pendingipdiscovery=`*`dhcp`*`|` *`static`* set /SP/network commitpending=true **Related Information**: • DNS Configuration Properties

Table 4-15 (Cont.) Network Connectivity Enhanced Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
IPv4 DHCP Client ID (`dhcp_clientid=`)	None	*None*|*SysID* 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 `system_identifier` property under the `/SP` 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 /SP/network dhcp_clientid=`*`none`*`|`*`sysid`* **Related Information**: • Assigning System Identification Information

Table 4-15 (Cont.) Network Connectivity Enhanced Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
IPv4 Network Address Netmask Address Gateway Address	Static IP Discovery Mode, Disabled	ipaddress=|ipnetmask=|ipgateway= **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. 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**: `set /SP/network pendingipaddress=`*`value`* `pendingipnetmask=`*`value`* `pendingipgateway=`*`value`* `set /SP/network commitpending=true` **Related Information**: • Input Format for IPv4 and IPv6 Addresses
IPv6 State (`/ipv6 state=`)	Enabled	*Enabled |Disabled* 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**: `set /SP/network/ipv6 state=`*`enabled`*`|`*`disabled`*

Table 4-15 (Cont.) Network Connectivity Enhanced Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
IPv6 Autoconfig (`/ipv6 autoconfig=`)	Stateless	disabled|stateless 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:** • 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 /SP/network/ipv6 autoconfig=`*`stateless`*`|`*`disabled`*

Table 4-15 (Cont.) Network Connectivity Enhanced Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
DHCPv6 Autoconfig (`/ipv6 autoconfig=`)	(none)	*DHCPv6_Stateless |DHCP_Stateful* The DHCPv6 Autoconfig property is disabled in Oracle ILOM by default. When this property is disabled, Oracle ILOM is prevented from learning the SP 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 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 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 dhcpv6_server_duid property. **CLI Syntax for DHCPv6 Autoconfig**: `set /SP/network/ipv6 autoconfig=`*`dhcpv6_stateless`*`|`*`dhcpv6_stateful`*
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 from another IPv6-enabled node on the same network. Oracle ILOM applies the following principles to build the Link-Local Address for the SP: • Oracle ILOM uses the SP 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 is unique. **CLI Syntax for Link-Local Address:** `show /SP/network/ipv6`

Table 4-15 (Cont.) Network Connectivity Enhanced Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
IPv6 Static IP Address (`/ipv6 static_ipaddress=`)	None	When the IPv6 state is enabled, network administrators can optionally assign a static IPv6 address to the SP. **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: *IPv6_address*/ *subnet_mask_length_in_bits*. 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 /SP/network/ipv6 pending_static_ipaddress=`*`ipaddress/ subnetmask`* `set /SP/network commitpending=true`
IPv6 Static Gateway (`/ipv6 static_ipgateway=`)	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 `/SP/network/ipv6 pending_static_ipgateway=`*`[user_specified_ipv6_gateway_address]`*
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/network/ipv6`

Table 4-15 (Cont.) Network Connectivity Enhanced Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
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. **Special Considerations**: • Oracle ILOM stores up 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/network/ipv6`

Table 4-15 (Cont.) Network Connectivity Enhanced Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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
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. 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 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 SP. **CLI Syntax for IPv4 Commit Pending Modification**: `set /SP/network state=`*`enabled`*`|`*`disabled`* `pendingipdiscovery=`*`static`*`|`*`dhcp`* `pendingipaddress=`*`value`* `pendingipgateway=`*`value`* `pendingipnetmask=`*`value`* `set /SP/network commitpending=true` **CLI Syntax for IPv6 Commit Pending Modifications:** `set /SP/network/ipv6 state=`*`enabled`*`|`*`disabled`* `pending_static_ipaddress=` *`value`*`/`*`subnet_mask_value`*`pending_static_ipgatewayaddress=` value `set /SP/network commitpending=true` **Related Information**: • Test IPv4 and IPv6 Connectivity

Table 4-16 DNS Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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	*Enabled |Disabled* 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. 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 /SP/clients/dns auto_dns=`*`enabled |disabled`*
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 /SP/clients/dns nameserver=`*`ip_address_1, ipaddress_2, ipaddress_3`*
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 /SP/clients/dns searchpath=` *`domain_1.com, domain_2.edu, and so on`*
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 /SP/clients/dns timeout=`*`n`* **Related Topic:** • Example Setup of Dynamic DNS
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. Optionally, network administrators can increase or decrease the default DNS Retries property value. **DNS Retries CLI Syntax:** `set /SP/clients/dns retries=`*`n`*
Save Button (web only)	N/A	**Web interface** – Changes made within the DNS Configuration page must be saved in Oracle ILOM before they can take affect.

Table 4-17 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	*SP* |*hostserver* The serial port Owner property is configurable on some Oracle servers. For further information, see Serial Management Port Owner. **CLI Syntax for Serial Port Owner:** `set /SP/serial/portsharing owner=`*`SP`*`|`*`hostserver`*

Host Serial Port
(`/host pendingspeed= flowcontrol= autobaud = disabled`)
	Baud Rate= 9600
	Flow Control= None
	Autobaud = Disabled
		`Baud Rate` = *9600* | `Flow Control` = *None* | `Autobaud = Disabled`
		The Host Serial Port properties are not configurable on all Oracle servers.
		The **Baud Rate** property enables you to set the Host Serial Port properties to match the internal serial communication settings between Oracle ILOM and the host serial port (serial port 0, COM1, or /dev/ttyS0)
		The **Flow Control** property controls the method of providing flow control.
		• Set to `None` (default) to specify no flow control.
		• Set to `Software` to enable the software to control the data flow (also known as Xon/Xoff).
		The **AutoBaud** property, as of Oracle ILOM firmware version 5.0.1, controls the method for automatically detecting and using the host baud rate value set on the host console. When disabled, Oracle ILOM uses Baud Rate property value set in Oracle ILOM. When enabled, Oracle ILOM automatically uses the host baud rate property value set on the host console.
		Note. 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/serial/host pendingspeed=`*`value`* `flowcontrol=`*`value`* `autobaud=`*`value`* `commitpending=true`

External Serial Port (`/external pendingspeed= flowcontrol=`)	Baud Rate= 9600 Flow Control= None	`Baud Rate` = *9600* |`Flow Control` = *None* 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**: `set /SP/serial/external pendingspeed=`*`value`* `commitpending=true`
Save Button (web only)	N/A	**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 by combining the product serial number with this prefix: SUNSP. For example, given a product serial number of 0641AMA007, the host name for a server SP would be SUNSP-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.

   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. Dynamic DNS dnssec-keygendnssec-keygenUsing 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:

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.

   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:

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

   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 4-18 Device Identification Configuration Properties

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
Host Name (`hostname=`)	Oracle branding string	The default Host Name is formed by concatenating an Oracle branding string, such as "ORACLESP-" 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:** `set /SP 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. **CLI Syntax for System Identifier**: `set /SP 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 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 system_location=`*`value`*

Table 4-18 (Cont.) Device Identification Configuration Properties

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
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 check_physical_presence=`*`true`*`|`*`false`* **Related Topic:** • Recover Preconfigured root Account or root Account Password (CLI only)
Save Button (web only)	N/A	**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 4-19 Oracle ILOM Clock Configuration Properties

User Interface Configurable Target and User Role:

- **CLI: `/SP/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/clock datetime=`*`MMDDhhmmYYYY`*

Table 4-19 (Cont.) Oracle ILOM Clock Configuration Properties

User Interface Configurable Target and User Role:

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

Property	**Default Value**	**Description**
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/clock timezones=`*`3_to_4_characters`*
Synchronize Time with NTP Server (`usentpserver=`)	Disabled	*Enabled|Disabled* 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 /SP/clock usentpserver=`*`enabled|disabled`*
NTP Server 1 (2) (`/SP/clients/ntp/server/`*`n`* `address=`*`<address>`*)	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 /SP/clients/ntp/server/1 address=`*`<address>`* `set /SP/clients/ntp/server/2 address=`*`<address>`* **Note.**Some server systems can support the configuration of more than two NTP servers.
Save Button (web only)	N/A	**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
- Recommended Practice for Spanning Tree Configurations
- Test IPv4 and IPv6 Connectivity

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.

- Troubleshooting IPv4 Connectivity Issues
- Troubleshooting IPv6 Connectivity Issues

Table 4-20 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 `/SP/network` 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 4-21 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: `https://[2001:db8:0:0:0:0:0:0]`
Unable to download a file using an IPv6 address.	Ensure that the IPv6 address in the URL is enclosed by brackets, for example: `load -source tftp://[2001:db8:0:0:0:0:0:0]/ desktop.pkg`

Table 4-21 (Cont.) Troubleshooting IPv6 Connectivity Issues

Problem	Suggested Resolution
Unable to access Oracle ILOM using IPv6 from a network client.	If on a separate subnet, try the following: • Verify that Oracle ILOM has a dynamic or static address (not just a Link-Local address). • Verify that the network client has 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 `/SP/network/ipv6` 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. Run `ping6` from the web or CLI. Or, run `traceroute` 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.
`bpdufilter`	Do not send or receive BPDUs on this interface.
`bpduguard`	Do not accept BPDUs on this interface.
`cdp`	Do not enable the discovery protocol on this interface.

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/network/test ping=device_ipv4_address_on network
    ```

```
set /SP/network/test ping6=device_ipv6_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:

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

Related Information:

- Network Connectivity Standard Configuration Properties

5

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
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)
Redirect a storage image file from a remote NFS or Samba server to the host server. For SPARC M7 or T7 Series Servers, manage the preinstalled Solaris Miniroot package.	• Redirecting an Image File From a Storage Device to the Host Server • Uploading a New Solaris Miniroot Package From SP to Host
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

Related Information

- Using the Oracle ILOM Remote System Console or Storage Redirection CLI
- Using the Oracle ILOM Remote System Console Plus
- Using Remote KVMS Securely

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 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.	Oracle servers 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	Using the Oracle ILOM Remote System Console or Storage Redirection CLI.

KVMS Console	Description	Firmware Versions	Managed Device	More Details
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 web interface, you can deploy serial or video redirection client sessions over the configured management network to the host server.	Oracle servers shipping with firmware version 3.2.1.x and later.	• x86 servers • Legacy SPARC servers (T7, M7, and T8). **Note**: The Remote Console Plus is not supported on M8 series servers **Note:** The S7-2 SPARC servers support serial redirection mode only.	Using the Oracle ILOM Remote System Console Plus.

KVMS Console	Description	Firmware Versions	Managed Device	More Details
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. 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.	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
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.	Oracle servers 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
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.	Oracle Servers shipping with firmware version 3.0.x and later.	All Oracle servers	Establishing a Host Serial Console Session to the Server (CLI)

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
- Dump Full Console History Contents to Remote Location
- Host Serial Console Log Properties

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 KVMS 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. Also, for SPARC multi-domain servers, see Host Status History Log for SPARC PDomains .
- 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:**
     In the Oracle ILOM CLI, type:

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

     For example:

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

   - **Dump Full Console History to a Remote URI Repository:**
     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 (Host Serial Console Log Properties or Host Status History Log for SPARC PDomains)

> **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 5-1 Host Serial Console Log Properties

<table>
<tr><td colspan="3"><b>User Interface Configurable Target and User Role:</b>
• <b>SP CLI: <code>/HOST/console</code> (or, /Servers/PDomain/PDomain_n/Host/console)</b>
• <b>User Role:</b>
<b>Admin (a) role is required to modify the <code>logging</code> and <code>escapechars</code> properties.</b>
<b>Console (c) role is required to modify the <code>line_count</code>, <code>pause_count</code>, and <code>start_from</code> properties.</b></td></tr>
<tr><th>Property</th><th>Default</th><th>Description</th></tr>
<tr><td><code>logging</code></td><td>enabled</td><td><i>enabled|disabled</i>
Set the <code>logging</code> 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:
<code>failed. could not get console history</code>
<b>CLI Syntax for</b> <code>logging</code> <b>:</b>
Single host server:
<code>set /HOST/console logging=<i>enabled|disabled</i></code>
Multi-domain host server:
<code>set /Servers/PDomain/PDomain_<i>n</i>/HOST/console logging=<i>enabled|disabled</i></code></td></tr>
</table>

Table 5-1 (Cont.) 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
`line_count`	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: `set /HOST/console line_count=`*`0 to 2048`* Multi-domain host server: `set /Servers/PDomains/PDomain_`*`n`*`/HOST/console line_count=`*`0 to 2048`*
`pause_count`	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: `press any key to continue or ???q' to quit` A value of 0 instructs Oracle ILOM to display the entire history log at once. **CLI Syntax for** `pause_count` **:** `set /HOST/console pause_count=`*`0 to 2048`*
`start_from`	end	*beginning|end* 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`*

Table 5-1 (Cont.) 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
`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`
		Multi-domain server:
		`show /Servers/PDomains/PDomain_` *n* `/HOST/console/history`

Table 5-2 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
- CLI and Web Host Storage Device Properties
- Uploading a New Solaris Miniroot Package From SP to Host

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

- 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.
- 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
(`mode`)
	disabled (for systems using SP firmware 3.2.4 or earlier)
	miniroot (for Oracle SPARC M7 and T7 series servers with Solaris OS image preinstalled and using SP firmware 3.2.5.5 or later)
		disabled |remote|miniroot
		The Mode property controls the Host Storage Device redirection behavior.
		• Disabled — Select Disabled to deactivate the host storage redirection service in Oracle ILOMRemote — 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 .
		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`*`]`

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
Server URI (`target_URI`)	(none)	*NFS, Samba, or SSHFS URI* **Note.** The SSHFS server URI 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 `/SP/services/ssh/keys/`*rsa* |*dsa* to the account for username and put it in the `.ssh/authorized_keys` file. For additional information about generating a public SSH key for user authentication, see, **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: `nfs://server:/path/file` **Sample NFS URI:** `nfs://198.51.100.2:/export/robert/biosimage.img` • To enter a URI using Samba, use the following format: `smb://server:/path/file` or `smb://server/path/file` **Sample Samba URI:** smb://198.51.100.2/robert/biosimage.img • To enter a URI using SSHFS, use the following format: `sshfs://host:/file_path` **Sample SSFS URI:** `sshfs://198.51.100.100:/export/john/example.img` **CLI Syntax for** `target_URI`**:** Single server: `set /SP/services/kvms/host_storage_device target_URI=`*`NFS_or_Samba_or_SSHFS_URI`* Multi-domain server: `set /Servers/PDomains/PDomain_`*`n`*`/SP/services/kvms/host_storage_device target_URI=`*`NFS_or_Samba_or_SSHFS_URI`*

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 Storage User Name (`username`)	(none)	*Samba Server username* or *SSHFS Server user name* 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: `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)	*Samba Server password* or *SSHFS Server password* 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`*

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

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.
		• 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:
		`show /SP/services/kvms/host_storage_device status`
		Multi-domain server:
		`show /Servers/PDomains/PDomain-n/SP/services/kvms/host_storage_device status`

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 the Oracle SPARC supported server (for instance, SPARC M7, T7. and T8 series server, S7-2L, or next generation SPARC). 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, as well as the Mode property that is described in CLI and Web Host Storage Device Properties.

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.

      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.`

      ii. In the Miniroot Update page, perform the following:

iii. Click either the Local File Browse button or specify a URL to locate the new Solaris Miniroot package.

iv. 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 `load_uri` 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 file_transfer_method can include: TFTP|FTP|SFTP|SCP|HTTP|HTTPS|Paste. For a detailed description of each file transfer method (excluding Paste), see Supported File Transfer Methods.

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

- Establishing an Oracle ILOM Remote System VNC Console Connection
- Troubleshooting the VNC Connection

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 1.2 encryption, must be installed.

    For instance, TigerVNC is a VNC viewer that supports the required TLS encryption in both Windows and Linux environments.
  - 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:

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

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 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:

     a. Click the Start menu, select TigerVNC.

     b. In the VNC Server property, type the server SP address (hostname or IP).

     c. 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
  ```

6

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 • Remote System Console First-Time Setup • Launching and Using the Oracle ILOM Remote System Console • Remote System Console Menu Options, Usage Considerations, and Toggle Keys • International Keyboard Support
Refer to these sections for setting up and using the text-based Oracle ILOM Storage Redirection CLI feature.	• Oracle ILOM Storage Redirection CLI • Storage Redirection CLI First-Time Setup • Launching and Using the Oracle ILOM Storage Redirection CLI • Storage Redirection Commands and Options • Resolving Warning Messages for Self-Signed SSL Certificate • Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate

Related Information

- 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.

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

- Remote System Console First-Time Setup
- Optionally Set a Lock Mode to Secure the Host Server Desktop
- Launching and Using the Oracle ILOM Storage Redirection CLI
- Remote System Console Menu Options, Usage Considerations, and Toggle Keys

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
- Configure Local Client KVMS Settings
- Register 32-Bit JDK Java Plug-In For Windows Edge Web Browser
- Register 32-Bit JDK Java Plug-In for Mozilla Firefox Web Browser
- Optionally Set a Lock Mode to Secure the Host Server Desktop

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 6-1 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
Java Runtime Environment	The Oracle ILOM Remote System Console requires the Java Runtime Environment to be either Java 8, Java 9, or later. To download the latest Java Runtime Environment, go to http://java.com .

Table 6-1 (Cont.) Requirements for Using Oracle ILOM Remote System Console

Set Up Requirement	Description
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.
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 Edge Web Browser • Register 32-Bit JDK Java Plug-In for Mozilla Firefox Web Browser
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. • **Video Redirection** – This option is available for Oracle's 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.
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 . 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.

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 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. If the State property is disabled, you will not be able to use the Oracle ILOM Remote System Console. **CLI Syntax for KVMS Service State**: • Single Sever SP: `set /SP/services/kvms servicestate=`*`enabled`*`|`*`disabled`* • Multi-domain server SP: `set Server/Pdomains/PDomain_`*`n`*`/SP/services/kvms 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 KVMS Mouse Mode**: • Single-server SP: `set /SP/services/kvms mousemode=`*`absolute`*`|`*`relative`* • Multi-domain server SP: `set /Servers/Pdomains/PDomain_`*`n`*`/SP/services/kvms mousemode=`*`absolute`*`|`*`relative`*

Property	Description

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 KVMS Display Quality:
	Single-server SP:
	`set /SP/services/kvms display_quality=YUV420| YUV444|VQ2|VQ4`
	Multi-domain server SP:
	`set /Servers/Pdomains/PDomain_n/SP/services/kvms display_quality=YUV420|YUV444|VQ2|VQ4`

Host Lock Mode (`lockmode=`)	For a description of the host lock properties, see Optionally Set a Lock Mode to Secure the Host Server Desktop .

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

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

1. On the Windows Client, open Windows Explorer File dialog.
2. In the Windows Explorer File 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.

      Click OK, and then launch the Oracle ILOM Remote System Console.

      For instructions, see Launching and Using the Oracle ILOM Remote System Console.

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.

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:

- Configurable Host Server Lock Options Configurable Host Server Lock Options
- Lock Host Desktop When Disconnecting a Remote KVMS Session

Table 6-2 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, scrl_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
- Remote System Console Menu Options, Usage Considerations, and Toggle Keys

Launch and Use the Oracle ILOM Remote System Console

Before You Begin

- Ensure that the requirements for first-time use have been met: Requirements for Using Oracle ILOM Remote System Console .

- 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 .
- 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, 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 .

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.

   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 a new KVMS session is manually added.

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 .

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.

5. To exit the Remote System Console, click Quit in the Redirection menu.

Related Information

- Requirements for Using the Oracle ILOM Remote System Console
- Remote System Console Menu Options, Usage Considerations, and Toggle Keys
- Optionally Set a Lock Mode to Secure the Host Server Desktop
- Storage Redirection CLI First-Time Setup

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
- Devices Menu Options
- Device Redirection Usage Considerations
- Keyboard Menu Options
- Toggle Key Sequence for Keyboard and Mouse Control
- International Keyboard Support

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

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
- Chinese
- Chinese -Traditional (Taiwan)
- English (US)
- Estonian
- French
- German
- Italian (IT)
- Korean
- Spanish
- Japan (JP) Note: Only in English mode.
- Russian
- Turkish

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
- Launching and Using the Oracle ILOM Storage Redirection CLI

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
- Register Java Plug-In for Windows Edge Browser and Start Service for First Time
- Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser
- Install the Storage Redirection Client
- Optionally Modify the Default Network Port 2121 for Storage Redirection

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 6-3 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 Java Download.

Table 6-3 (Cont.) Requirements for Using Oracle ILOM Storage Redirection CLI

Setup Requirement	Description
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 Edge Browser and Start Service for First Time • Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser
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
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

Register Java Plug-In for Windows Edge 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 File dialog.
2. In the Windows Explorer File 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
- Optionally Modify the Default Network Port 2121 for Storage Redirection

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 Edge Browser and Start Service for First Time
  – Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser.

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:
   - 00Click “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
- Launching and Using the Oracle ILOM Storage Redirection CLI

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
- Interactive and Non-Interactive Shell Syntax
- Storage Redirection Commands and Options

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: Requirements for Using Oracle ILOM Storage Redirection CLI.
- 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

  Storage Redirection Commands and Options

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. To launch the Storage Redirection CLI using an interactive shell mode, perform these steps: **a.** In the command-line interface, navigate to the directory where the storage redirection client (`StorageRedir.jar`) is installed using the `cd` command. For example: `cd` *my_settings/storage_redirect_directory* **b.** Enter the following command to launch the Storage Redirection CLI: `java -jar StorageRedir.jar` For example: `C:\Documents and Settings\` *redirectstorage* `java -jar StorageRedir.jar` The <*storageredir*> 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 c: you must specify C: instead of c:. **Tip:** Enter only one space before `java` and one space before and after `-jar`. Otherwise, the `java -jar StorageRedir.jar` command will fail. **Related Information:** • Interactive and Non-Interactive Shell Syntax

Shell Mode	Description and Procedure
Non-interactive shell mode	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: **a.** In the command-line interface, enter the command to launch the Storage Redirection CLI (`java -jar StorageRedir.jar`) at the shell prompt ($). For example: `$java -jar StorageRedir.jar` **Note** – If you do not have a `JAVA_HOME` environment configured, you might need to use the full path to your Java binary. For example, if your JDK package was installed under `/home/user_name/jdk`, then you would type:`/home/user_name/jdk/bin/java -jar ...` **b.** 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 (`-jar StorageRedir.jar`) from a local command window or terminal. **Tip:** Enter only one space before and after `-jar`. Otherwise, the `java -jar StorageRedir.jar` command will fail. **Related Information:** • Interactive and Non-Interactive Shell Syntax • Storage Redirection Commands and Options

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
   - Interactive and Non-Interactive Shell Syntax

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
- Interactive and Non-Interactive Shell Syntax

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
   - Interactive and Non-Interactive Shell Syntax

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_defult_storageredir_port] [-a
   yes/no] remote_SP
   ```

   For command descriptions and shell mode syntax, see these topics:

   - Storage Redirection Commands and Options
   - Interactive and Non-Interactive Shell Syntax

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

- Storage Redirection Commands
- Storage Redirection Command Options
- Storage Redirection Sub-Commands
- Storage Redirection Sub-Command Options

Table 6-4 Storage Redirection Commands

Command Name	Description
`java -jar StorageRedir.jar`	The `java -jar` command is used to launch the storage redirection client (`StorageRedir.jar`) from a command window or terminal.
`storageredir`	The `storagedir` command performs all storage redirection operations.

Table 6-5 Storage Redirection Command Options

Option Name	Description
`– h`	The `–h` command option displays the command-line Help information.
`– v`	The `–v` command option displays the Java command version information.

Table 6-6   Storage Redirection Sub-Commands

Sub-Command Name	Description
`list`	The `list` sub-command provides a list of the currently active storage redirections on one or all remote SPs. **Syntax usage example:** `storageredir list [-p` *`storageredir_port`*`] [`*`remote_SP`*`]`
`start`	The `start` 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:** `storageredir start -r` *`redir_type`* `-t` *`redir_type_path`* `-u` *`remote_username`* `[-s` *`remote_user_password`*`]` `[-p` *`storageredir_port`*`]` *`remote_SP`* **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.

`stop`	The `stop` 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:
	`storageredir stop -r` *`redir_type`* `-u` *`remote_username`*
	`[-s` *`remote_user_password`*`] [-p` *`storageredir_port`*`]`
	`remote_SP`
	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.

`test-service`	The `test-service` sub-command verifies whether the Storage Redirection service connection is active on the local host. **Syntax usage example:** `storageredir test-service [-p` *`storageredir_port`*`]`
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 6-7   Storage Redirection Sub-Command Options

Sub-Command Option Name	Description
`-r` *redir_type*	The `-r` *redir_type* identifies the type of storage media being redirected. Valid device values for *redir_type* 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` *redir_type_path*	The `-t` *redir_type_path* 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` *remote_username*	The `-u` *remote_username* 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` *remote_user_password*	The `-s` *remote_user_password* 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`
yes/no
	The `-s yes/no` 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.
	As of Oracle Firmware 3.2.5.3, the `-syes/no`option applies when issuing the `Start` and `Stop` sub-commands.
	Syntax usage examples:
	`-s yes`
	or
	`-s no`

`-p` *storageredir_port*	The `-p` *storageredir_port* identifies the storage redirection communication port on the local host. The default port provided is 2121. **Syntax usage example:** `-p 2121`

7

Using the Oracle ILOM Remote System Console Plus

> **Note:**
>
> The Oracle ILOM Remote System Console Plus is available on all Oracle servers 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 • Remote System Console Plus First-Time Setup
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) • Set a Lock Mode to Secure the Host Server Desktop (Optional)
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 • Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards • Toggle Button, Virtual Keys, and Status Icons • Resolving Warning Messages for Self-Signed SSL Certificate • Resolving Warning Messages for Custom Certification Authority (CA) SSL Certificate

Related Information

- Using Remote KVMS Securely
- Using the Oracle ILOM Remote System Console Plus

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.

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).

  > **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
- Set a Lock Mode to Secure the Host Server Desktop (Optional)
- Launching and Using the Oracle ILOM Remote System Console Plus
- Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards

> **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.

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
- Configure Local Client KVMS Settings
- Modify KVMS Maximum Client Session Count (Optional)
- Set a Lock Mode to Secure the Host Server Desktop (Optional)

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:

- Requirements for Using Oracle ILOM Remote System Console Plus

Table 7-1 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 . **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
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 • Set a Lock Mode to Secure the Host Server Desktop (Optional)
	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 in is 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. 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. **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

Table 7-1 (Cont.) Requirements for Using Oracle ILOM Remote System Console Plus

Set-Up Requirement	Description
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 8, Java 9, or later. To download the latest Java Runtime Environment, go to Java Download.
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 .
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) .
Communication TCP/IP Ports Required	The Oracle ILOM Remote System Console Plus uses the following TCP/IP communication ports by default: • 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 .

Table 7-1 (Cont.) Requirements for Using Oracle ILOM Remote System Console Plus

Set-Up Requirement	Description
Keyboard Support	See International Keyboard Support .
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 . 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, seeResolving Warning Messages for Self-Signed SSL Certificate .

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) .
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) .

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	**a.** Navigate to the Remote Console > KVMS page. **b.** 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. **c.** 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. **d.** Click Yes to proceed; or, click No to cancel the operation.
CLI	**a.** Type: `set /SP/services/kvms max_session_count=`[*1*|*2*|*3*|*4*(default)] 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. **b.** 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.

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:

- Configurable Host Server Lock Options
- Lock Host Desktop When Disconnecting a Remote KVMS Session

Table 7-2 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:
  1. **set /SP/services/kvms lockmodifiers=value**
  2. **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, scrl_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

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
- Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards
- Toggle Button, Virtual Keys, and Status Icons

Launch and Use the Oracle ILOM Remote System Console Plus

Before You Begin

- Ensure that the requirements for first-time use have been met: Requirements for Using Oracle ILOM Remote System Console Plus.
- 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 KVMS 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 .

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).

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

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.

> **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.

   > **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
- Remote System Console Plus Menu Options, Usage Considerations, and Supported Keyboards
- Set a Lock Mode to Secure the Host Server Desktop (Optional)

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
- Preference Menu Options
- Help Menu Options
- International Keyboard Support

KVMS Menu Options

Menu Option	Description
Storage	The Storage option when selected opens the Storage Device dialog box.

Menu Option	Description
-	**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: `Unable to open the drive exclusively`. 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.
-	**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.

Menu Option	Description
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). **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.

Preference Menu Option	Description
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. 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)
- Dutch (NL)
- Dutch Belgium (NL)
- English (US)
- Finnish (FI)
- French (FR)
- French Belgium (FR)
- German (DE)
- German (Swiss)
- Italian (IT)
- Japan (JP) Note: Only in English Mode.
- Norwegian (NO)
- Portuguese (PT)
- Spanish (ES)
- Swedish (SV)
- Turkish - F (TR)
- Turkish - Q (TR)
- United Kingdom (EN)

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 • 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.

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.

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 an administrator. To start a command prompt as an administrator on a Windows systems: 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
  ```

8

Configuring Host Server Management Actions

Description	Links
Refer to this section for descriptions SP configurable properties for host power control.	• Controlling Host Power to Server • Setting the External Power Button Override Policy on x86 Servers
Refer to this section for descriptions of SP configurable diagnostic properties.	• Setting Diagnostic Tests to Run
Refer to this section for descriptions of x86 SP configurable properties for next boot device.	• Setting Next Boot Device on x86 Host Server
Refer to this section for descriptions of SPARC SP properties for host control.	• Setting Host Control and Boot Properties on SPARC Host Server
Refer to this section for descriptions of SPARC SP configurable boot mode properties for OpenBoot and LDoms.	• Overriding SPARC Host Boot Mode
Refer to this section for instructions on how to set Verified Boot properties	• Configuring SPARC Verified Boot Properties
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
Refer to this section for descriptions of SPARC SP configurable property values for the host KeySwitch state.	• Setting SPARC Host KeySwitch State
Refer to this section for descriptions of SPARC SP configurable property values for the host TPM state.	• Setting SPARC Host TPM State
Refer to this section for descriptions of SPARC SP configurable property values for host state capture on error.	• Setting SPARC Host State Capture
Refer to this section for descriptions of SPARC host I/O reconfiguration property values.	• Managing SPARC Host I/O Reconfiguration Policy
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
Refer to this section for instructions on how to redirect host output to rear VGA port.	• Redirecting Host Output to Rear VGA Port

Related Information

- Maintaining x86 BIOS Configuration Parameters

Controlling Host Power to Server

Oracle ILOM provides a set of parameters that enables system administrators to control the power state of a host server.

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 8-1 Remote Power Control Commands for Host Managed Devices

User Interface Configurable Target and User Role:

- **CLI: `[`*`command`*`] /System` (or for multi-domain servers: [*command*] /Servers/PDomains/PDomain_*n* /HOST)**
- **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: `reset /System` • SPARC: `reset -force /System`	• 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	• `reset /System`	• SPARC server only	Use Graceful Reset to gracefully shut down the host operating system prior to power-cycling the managed server.
Immediate Power Off	• `stop -force /System`	• Any managed server	Use Immediate Power Off to directly shut down the power to the managed device.
Graceful Shutdown and Power Off	• `stop /System`	• Any managed server	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	• `start /System`	• Any managed server	Use Power On to apply full power to the managed device.
Power Cycle	• `stop /System` • `start /System`	• 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
- Navigating the Command-Line Interface (CLI) Namespace Targets

Setting the External Power Button Override Policy on x86 Servers

Oracle ILOM, as of firmware version 5.0.1, enables administrators to enable or disable the use of the external power button on all standard Oracle x86 Servers with the exception of these models: G5, G5PLUS, X7-GX, X8-GX. By default, this policy is only configurable from the Oracle ILOM CLI. For further details about setting this policy in the Oracle ILOM CLI, see the following table.

Table 8-2   External Power Button Override Policy Configuration Property

User Interface Configurable Target and User Role:

- **SP CLI: SP/policy**
- **User Role: Admin (a) role (required to modify the property for the External Power Button Override Policy).**

Notes:

- **As of Oracle ILOM firmware 5.0.1, this property is available for configuration on all standard Oracle x86 Servers with the exception of these models: G5, G5PLUS, X7-GX, X8-GX.**

Property	Default	Description
`EXTERNAL_POWER _BUTTON _OVERRIDE =`	*Disabled **Note:** *This property is Disabled by default on supported Oracle x86 Enterprise Servers. This property is Enabled by default on supported Oracle x86 Cloud Servers.	*Disabled* | *Enabled* • Disabled – When Disabled, pressing the external power button on the x86 server will power ON or OFF the host power. • Enabled – When Enabled, the external power button is disabled to prevent accidental server power off. Pressing the external power button on the x86 server will not power ON or OFF the host power. The power must be controlled through the Oracle ILOM Web or CLI interface. **Note.** When the External Power Button Override property is modified, an event appears in the Oracle ILOM Audit log. **CLI Syntax for External Power Button Override Policy**: `set /SP/policy EXTERNAL_POWER_BUTTON_OVERRIDE =` *disabled* | *enabled*

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:

- x86 Server SP Diagnostic Properties x86 Server SP Diagnostics Properties
- Legacy SPARC Systems Host Diagnostic Properties (M6, M5, T5, and earlier) Legacy SPARC Systems Host Diagnostic Properties (M6, M5, T5 and earlier)
- Newer SPARC Systems Host Diagnostic Properties (M7, T7, and later) Newer SPARC Systems Host Diagnostic Properties (M7, T7 and later)
- Newer SPARC Systems SP Diagnostic Properties (M7, T7, and later) Newer SPARC Systems SP Diagnostic Properties (M7, T7 and later)

Table 8-3 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 mode=*disabled* |*enabled* | *extended*|*manual*)	Disabled	*Disabled*| *Enabled* |*Extended* |*Manual* • 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. **CLI Syntax for Diagnostics on Boot State:** `set /HOST/diag mode=` *`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 8-4 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	*Power-On*| *HW-Change*|*Error-Reset* 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* 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*

Table 8-4 (Cont.) 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 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:** `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	*Off |Normal* 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 8-5 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=`)
(`default_verbosity=`)
	Level = Off
	Verbosity = Normal
		Level: *Off* | *Min* | *Max*
		Verbosity: *Normal* | *None* | *Min* | *Max* |*Debug*
		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.
		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 – (*The Debug setting is no longer supported as of Oracle ILOM firmware version 3.2.6 or SPARC SW 9.7.x.*) 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*

Table 8-5 (Cont.) 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

Error Reset Level and Verbosity
(`error_level=`)
(`error_verbosity=`
)
	Level = Max
	Verbosity = Normal
		Level: *Off* | *Max* |*Min*
		Verbosity: *Normal* | *None* | *Min* | *Max*
		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.
		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
		`set /HOST/diag error_reset_level=` *off*|*min*|*max* `verbosity_level=` *normal\none*|*min*|*max*
		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*

Table 8-5 (Cont.) 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

HW_Change Level and Verbosity
(`hw_change_level=`)
(`hw_change_verbosity=`)
	Level = Max
	Verbosity = Normal
		Level: *Off* |*Min* |*Max*
		Verbosity: *None* | *Min* | *Max* | *Debug*
		• 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.
		Verbosity Max – When enabled, all the POST step debugging output is printed to system console.
		Verbosity Debug – (*The Debug setting is no longer supported as of Oracle ILOM firmware version 3.2.6 or SPARC SW 9.7.x.*) 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 8-6 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 (`default_level=`)	Level = Off	Level: *Off* | *Min* | *Max* 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 Off. **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. • 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: *Max* | *Min|Off* 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. 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
- Navigating the Command-Line Interface (CLI) Namespace Targets

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 8-7 Set Next Boot Device Property on x86 Managed Server

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

Default (Use BIOS Settings)
(`boot_device=default`)
	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:
	`set /HOST/boot_device=default`
	Multi-domain server:
	`set /Servers/PDomains/PDomain_n/HOST/ boot_device=default`

PXE (`boot_device=pxe`)	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: **set /HOST/boot_device=pxe** Multi-domain server: `set /Servers/PDomains/PDomain_n/HOST/ boot_device=pxe`

Table 8-7 (Cont.) Set Next Boot Device Property on x86 Managed Server

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
(`boot_device=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.
	CLI Syntax:
	Single server:
	`set /HOST/boot_device=floppy`
	Multi-domain server:
	`set /Servers/PDomains/PDomain_n/HOST/ boot_device=floppy`

Table 8-7 (Cont.) Set Next Boot Device Property on x86 Managed Server

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

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
- Navigating the Command-Line Interface (CLI) Namespace Targets

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 8-8 Host Control Information and Boot Properties on SPARC Managed Server

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
Host Control Information `/HOST`	Read-only properties	View SPARC server host control information for: • 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 (`alert_forwarding=`)	Disabled	Disabled (default) | Enabled 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. **CLI Syntax for Alert Forwarding** `set /HOST alert_forwarding` *`disabled`* `|` *`enabled`*

Table 8-8 (Cont.) Host Control Information and Boot Properties on SPARC Managed Server

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
Auto Restart Policy (`autorestart=`)	Reset	*Reset* |*Dump Core*|*None* 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`*

Table 8-8 (Cont.) Host Control Information and Boot Properties on SPARC Managed Server

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
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. In addition, this property is available for configuration on SPARC T4 servers as of Oracle ILOM firmware release 3.2.6.7. **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 harware-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 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`*

Table 8-8 (Cont.) Host Control Information and Boot Properties on SPARC Managed Server

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
Auto Run on Error (`autorunonerror=`)	Poweroff	*None*| *Powercycle*| *Poweroff* **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`* For earlier Oracle SPARC servers, like the T-3 Series servers, the properties for `autorunonerror=`*`true`*`|`*`false`* . When set to *`true`* , the host is power cycled if a fatal error is encountered. When set to *`false`* (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	*None*|*Reset* Set to instruct Oracle ILOM whether to restart the SPARC server if the system times out. **CLI Syntax for Boot Restart Policy**: `set /HOST bootrestart=` *`reset`*`|`*`none`*

Table 8-8 (Cont.) Host Control Information and Boot Properties on SPARC Managed Server

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
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
- Navigating the Command-Line Interface (CLI) Namespace Targets

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 8-9 Host Boot Mode Properties for Host SPARC Server

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
State `(state=)`	Normal	*Normal* | *Reset NVRAM* 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: `set /HOST/bootmode state=` *normal*|*reset_nvram* • For multi-domain server SP, type: `set /Servers/PDomains/PDomain_`*n* `/HOST/bootmode state=` *normal*|*reset_nvram*

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.
		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`

Table 8-9 (Cont.) Host Boot Mode Properties for Host SPARC Server

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**

Script
(`script=`)
		Up to 1000 bytes in length.
		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 (`config=`)	Factory-default	*Factory-default* | *Valid LDOM 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/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**: `set /HOST/bootmode config=` *factory-default|valid_LDOM_configuration*

Related Information

- Navigating the Web Interface
- Navigating the Command-Line Interface (CLI) Namespace Targets

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 Verified Boot Properties.

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 8-10 Verified Boot Properties

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
Boot Policy (`boot_policy`)	none	*none |warning|enforce* • 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: `set /Host/verified_boot boot_policy=` *none|warning|enforce* Multi-domain host server: `set /Servers/PDomains/PDomain_`*n*`/HOST/verified_boot boot_policy=` *none|warning|enforce* **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 *Oracle ILOM Feature Updates and Release Notes*.
System Certificates (`/system_certs/1`)		View the `system_certs/1` target for details about pre-installed certificate files, such as the issuer and subject of the file.

Table 8-10 (Cont.) Verified Boot Properties

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
User Certificates (`/user_certs/`*n*)		Load up to five custom certificate files to verify Solaris kernel modules other than `unix` and `geunix`. View the `user_certs/n` 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: `set /Host/verified_boot/user_certs/`*`n`* `load_uri=`*`protocol`*`://`*`certificate_URI`* Multi-domain host server: `set /Servers/PDomains/PDomain_`*`n`*`/Host/verified_boot/user_certs/`*`n`* `load_uri=`*`protocol`*`://`*`certificate_URI`* Where *n* 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 **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 *n* 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:

- View Logical Domain Configurations Detected for Host SPARC Server View Logical Domain Configurations Detected for Host SPARC Server
- Host Domain Configurable Properties for Host SPARC Server Host Domain Configurable Properties for Host SPARC Server

Table 8-11 View Logical Domain Configurations Detected for Host SPARC Server

User Interface Configurable Target:

- **SP CLI: `/HOST/domain/configs`**
- **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 (`show /HOST/domain/configs`)**

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 8-12 Host Domain Configurable Properties for Host SPARC Server

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
Auto-Run (`auto-boot=`)	Enabled	*Enabled* |*Disabled* 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: `set /HOST/domain/control auto-boot=` *enabled|disabled* For multi-domain server SP, type: `set /Servers/PDomains/PDomain_`*n*`/HOST/domain/control auto-boot=` *enabled|disabled*

Table 8-12 (Cont.) Host Domain Configurable Properties for Host SPARC Server

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 (`boot_guests=`)	Enabled	*Enabled* |*Disabled* 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: `set /HOST/domain/control boot_guests=` *enabled|disabled* For multi-domain server SP, type: `set /Servers/PDomains/PDomain_`*`n`*`/HOST/domain/control boot_guests=` *enabled|disabled*

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 8-13 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 (`keyswitch_state=`)	Normal	*Normal* |*Standby* |*Diag*|*Locked* • 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
- Navigating the Command-Line Interface (CLI) Namespace Targets

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.

- TPM Property Values for Host SPARC Servers TPM Property Values for Host SPARC Server
- TPM Property Values for Legacy Host SPARC Servers TPM Property Values for Legacy Host SPARC Servers

Table 8-14 TPM Property Values for Host SPARC Servers

<table>
<tr><td colspan="3">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.</td></tr>
<tr><th>Property</th><th>Default</th><th>Description</th></tr>
<tr><td>TPM
(mode=)
(forceclear=)</td><td>Disabled ('off')</td><td>Mode = activated (enabled)| deactivated (disabled) | off (default); Forceclear= false (default) | true
• 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:
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</td></tr>
</table>

Table 8-15 TPM Property Values for Legacy Host SPARC Servers

<table>
<tr><td colspan="3"><b>User Interface Configurable Target and User Role:</b>
• <b>SP CLI: <code>/HOST/tpm</code></b>
• <b>Web: Host Management > TPM > TPM Settings</b>
• <b>User Role: Reset and Host Control (r) role (required to modify TPM property).</b>
<b>Requirements:</b>
• <b>The host SPARC server must be running an Oracle Solaris Operating System version that supports TPM.</b>
• <b>To apply TPM property modifications in the web interface, you must click Save.</b></td></tr>
<tr><th>Property</th><th>Default</th><th>Description</th></tr>
<tr><td>TPM
(<code>enable=</code>)
(<code>activate=</code>)
(<code>forceclear=</code>)</td><td>Disabled ('false')</td><td>Enable=<i>false</i> | <i>true</i>; Forceclear=<i>false</i> | <i>true</i>; Activate=<i>false</i> | <i>true</i>
To enable the SPARC server TPM device on the next host power-on event, set the properties for Enable and Activate to 'true'.
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'.
Note: The Forceclear property is automatically set to 'false' after the next host power-on event.
<b>CLI Syntax to Set TPM Properties</b>:
<code>set HOST/tpm enable=[<i>true</i>|<i>false</i>] activate=[<i>true</i>|<i>false</i>] forceclear=<i>false</i>|<i>true</i></code></td></tr>
</table>

Related Information

- Navigating the Web Interface
- Navigating the Command-Line Interface (CLI) Namespace Targets

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 8-16 Host State Capture Properties for SPARC Server

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
State Capture on Error (state_capture_on_error=)	enabled	*enabled | disabled* The 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 (`state_capture_mode=`)	default	**Note:** The State Capture Mode property only applies to SPARC M5, M6 and T5 systems. This property is not available for configuration on SPARC M7, T7, S7, M8, or T8 systems. *redstate_scandump* | *fatal_scandump* | *default* 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 - When a Fatal Reset error occurs, error register and scandump data is collected and saved to Oracle ILOM. For all other errors, only error register data is recorded. • redstate Scandump - 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*

Table 8-16 (Cont.) Host State Capture Properties for SPARC Server

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
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
- Navigating the Command-Line Interface (CLI) Namespace Targets

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 8-17 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 (`ioreconfigure=`)	true	*false|true|add_only* • 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:** When the control domain creates its first guest domain, the IO Reconfigure Policy property is automatically set to false. • 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: `set /SP/Host ioreconfigure=` *true|false|add_only* For SPARC multi-domain server SP, type: `set /Servers/PDomains/PDomain_n/Host ioreconfigure=` *true|false|add_only*

Related Information

- Navigating the Web Interface
- Navigating the Command-Line Interface (CLI) Namespace Targets

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
- PDomain and DCU Assignments

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.
- Set DCU Failover Control for System

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.
- 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:
     a. 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).
     b. 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.

    - *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.

DCU Status States

For a list of possible health status states for logical DCU-host configurations, see the following table.

Table 8-18 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 8-19 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: `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
- Assign Or Unassign DCUs To a PDomain Host
- Change Controlling PDomain-SPP for Host (Failover)

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 8-20   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	*Disabled* | *Enabled* • 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
- Navigating the Command-Line Interface (CLI) Namespace Targets

9

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
Refer to this section for configuration information for enabling Automatic Service Requests.	• Managing Automatic Service Requests
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

Related Information

- Managing Oracle ILOM Log Entries
- Managing SNMP Trap Alerts Using the Oracle ILOM
- SNMP Configuration Properties

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
- Configure and Test Alert Notification (IPMI PET, SNMP, or Email)
- Disable Alert Notification (IPMI PET, SNMP, or Email)
- Configure SMTP Client for Email Alerts

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 9-1 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 *Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 5.0.x* • *IPMI Alerts* in *Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 5.0.x*
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.

Table 9-1 (Cont.) Alert Notification Configuration Properties

Property	Requirement	Description
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. 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: *Minor*, *Major*, *Critical*, or *Down*.
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 SMPT 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 (““).

Table 9-1 (Cont.) Alert Notification Configuration Properties

Property	Requirement	Description
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 or User Name	Optional for SNMP Alerts	System administrators can optionally specify an SNMPv1 or 2c community string or an SNMPv3 user name. **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.

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.
- 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 SNMP Configuration Properties.
- 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 Alert Notification Configuration Properties .
   - **CLI:**
     Type the following to set the required alert properties:

     ```
     set /SP/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 Alert Notification Configuration Properties .
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/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:

- Alert Notification Configuration Properties
- Configure SMTP Client for Email Alerts
- SNMP Configuration Properties
- Managing Oracle ILOM Log Entries
- Managing SNMP Trap Alerts Using the Oracle ILOM

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).

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/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 SMPT 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/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)

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
- Manage Endpoint SSL Certificate Information
- Send an ASR Test or Heartbeat Message
- ASR Configuration Properties

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 ASR Client Properties.
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.
- 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.
     - **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 9-2 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. • **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.

Table 9-2 (Cont.) ASR Client Properties

Property	Default	Description
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=`)	Oracle Transport LinK	provided transfer link (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** • *https|http* `://` *asr_manager_host* • *https|http* `://` *asr_manager_host:port_number* `/asr` **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. 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 .

Table 9-2 (Cont.) ASR Client Properties

Property	Default	Description
Strict Certificate Mode	Enabled	Enabled (default) | Disabled 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 (`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 My Oracle Support **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 (`proxy-host=`) (`proxy-user=`) (`proxy-password=`)	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 *not* 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/clients/syslog destination_ip=syslog_server_ip`

Related Information:

- Managing Oracle ILOM Log Entries

10 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
Refer to this section to manage the Device Monitoring configuration.	• Setting Device Monitoring Configuration Properties

Related Information

- Setting Power Alert Notifications and Managing System Power Usage

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 10-1 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=`)	*Disabled* (default) |*Enabled* 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 *not* 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=`)	*Disabled* (default) |*Enabled* 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 *not* 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=`)	*Disabled* (default) |*Enabled* 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`*

Table 10-1 (Cont.) 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
Set Low Line AC Override Mode Policy (x86 server only) (`LOW_LINE_AC_OVERRIDE_MODE=`)	*Disabled* (default) |*Enabled* 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. **CLI Syntax for Set Low Line AC Override Mode Policy:** `set /SP/policy LOW_LINE_AC_OVERRIDE_MODE=[`*`enabled`*`|`*`disabled`*`]` **Note:** The `LOW_LINE_AC_OVERRIDE_MODE` property is *not* 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`*`]` **Note:** The `LOW_LINE_AC_OVERRIDE_MODE` property is *not* configurable on all x86 servers.
Set Parallel Boot (Supported on most SPARC T series servers and SPARC 7-2 series servers) (`PARALLEL_BOOT=`)	*Enabled* (default) |*Disabled* 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 *not* 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=`)	*Disabled* (default) |*Enabled* **Note:** The `VGA_REAR_PORT` property is *not* 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`*

Table 10-1 (Cont.) 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
Set Enhanced PCIe Cooling Mode (x86 server only) (`ENHANCED_PCIE_COOLING_MODE=`)	*Disabled* (default) |*Enabled* Set to allow the host to poweron independently of ILOM Enable this policy on an Oracle x86 server PCEI 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. **CLI Syntax for Set Enhanced PCIe Cooling Mode:** `set /SP/policy ENHANCED_PCIE_COOLING_MODE=`*`enabled`*`|`*`disabled`* **Note:** The `ENHANCED_PCIE_COOLING_MODE` property is *not* configurable on all x86 servers.
Enable a Cooldown Period Before Host Shuts Down (SPARC server only) (`HOST_COOLDOWN=`)	*Disabled* (default) |*Enabled* 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 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:** `set /SP/policy HOST_COOLDOWN=`*`enabled`*`|`*`disabled`*

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.

Before updating RAID HBA, NVMe, or other optional device firmware, it is recommended to suspend the Oracle ILOM Device Monitor feature if it is applicable for the server and if the feature is enabled. Monitored upgradable devices can create FMA faults if the firmware update contains updates for these devices. After the device firmware update has completed, re-enable device monitoring. If the SP reboots after the firmware update procedure or the server is power cycled, device monitoring is reset to the enabled state, which is the default setting. If the firmware update procedure cannot be modified within a workflow, mitigate the FMA fault first on the monitored device and then on Oracle ILOM before proceeding with the update.

For a description of the device monitoring configuration properties, see the following table:

Table 10-2 Configurable Device Monitoring Properties

<table>
<tr><td colspan="2"><b>User Interface Configurable Target and User Role:</b>
• <b>CLI: <code>/SP/services/device_monitor</code></b>
• <b>Web: System Management > Device Monitor</b>
• <b>User Role: admin (a) (required for all property modifications)</b></td></tr>
<tr><th>System Management Policy</th><th>Description</th></tr>
<tr><td>Service State
(<code>servicestate=</code>)</td><td><b>Note:</b> 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 (<code>show /System/Open_Problems</code>).
• 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.
<b>CLI Syntax for Device Monitor Service State:</b>
<code>set /SP/services/device monitor servicestate=</code> <code><i>enabled</i> | <i>disabled</i> | <i>suspended</i></code></td></tr>
<tr><td>Polling Interval
(<code>polling_interval=</code>)</td><td>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).
<b>CLI Syntax for Device Monitor Polling Interval:</b>
<code>set /SP/services/device_monitor polling interval=</code> <code>[<i>30 to 600</i>]</code></td></tr>
</table>

11

Setting Power Alert Notifications and Managing System Power Usage

Description	Links
Refer to this section for descriptions of SP configurable properties for power consumption alert notifications.	• Setting Power Consumption Alert Notifications
Refer to these sections for descriptions of SP configurable properties for managing system power usage.	• Setting SP Power Limit Properties • Setting SP Advanced Power Capping Policy to Enforce Power Limit • Setting SP Power Management Settings for Power Policy (SPARC)

Related Information

- Real-Time Power Monitoring Through Oracle ILOM Interfaces
- Configuring Alert Notifications, Service Requests, or Remote Logging

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.

For details about configuration properties for power notification thresholds, see the following table.

Table 11-1 Power Consumption Notification Threshold Configuration Properties

<table>
<tr><td colspan="3"><b>User Interface Configurable Target and User Role;</b>
• <b>SP CLI: /SP/powermgmt</b>
• <b>Web: Power Management > Consumption > Notification Threshold 1 | 2</b>
• <b>Admin (a) role (required to modify threshold properties).</b></td></tr>
<tr><td colspan="3"><b>Requirements:</b>
• <b>To apply threshold property modifications in the web interface, you must click Save.</b>
• <b>Email alert notification properties must be configured in Oracle ILOM.</b></td></tr>
<tr><th>Property</th><th>Default</th><th>Description</th></tr>
<tr><td>Notification Threshold 1 and 2
(threshold1=<i>n</i> |threshold2=<i>n</i>)</td><td>Disabled</td><td><i>Disabled</i>| <i>Enabled</i>
• Disabled – When disabled, the Notification Threshold property state and wattage property value (<i>0</i>) 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.
<b>CLI Syntax for Power Consumption Notification Threshold</b>
<code>set /SP/powermgmt threshold1=[<i>0 to 65535</i>] threshold2=[<i>0 to 65535</i>]</code>
<b>Related Information:</b>
• Configuring Alert Notifications
• Power Consumption Terminology and Properties</td></tr>
</table>

Setting SP Power Limit Properties

Oracle ILOM provides SP configurable properties for limiting power use on a managed server. These 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 setting an SP Power Target Limit, see the following procedure.

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. 2. 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). 3. Enable the activation state for Power Limiting. The Power Limiting state must be enabled for Oracle ILOM to activate the target power limit configuration. 4. Click Save to apply the changes. 5. To enforce the set power limit property on the SP, see Set Advanced Power Capping Policy .
CLI	1. Type: `set /SP/powermgmt/budget pending_power_limit=value pendingactivation_state=enabled commit_pending=true` Where *value* 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). 2. To enforce the set power limit property on the SP, see Set Advanced Power Capping Policy .

Related Information

- Monitoring Power Allocations
- Setting SP Advanced Power Capping Policy to Enforce Power Limit
- Getting Started With Oracle ILOM

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.
- 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	1. Click Power Management > Power Limit. 2. 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. 3. 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. 4. Click Save to apply the changes.

Oracle ILOM Interface	Set Power Capping Policy (Soft Cap, Hard Cap, and Violation Actions) Procedure

CLI	**1.** To set a Soft Cap or Hard Cap value for the Power Capping Policy type:
	`set /SP/powermgmt/budget pendingtimelimit=`*`default|integer between 1 and 99999|0`* `commit_pending=true`
	Where:
	default or *integer between 1 and 99999* 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 `timelimit` property (default, 10 seconds).
	- or -
	0 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 `violation_actions`, type:
	`set /SP/powermgmt/budget pendingviolation_actions=`*`none|hardpoweroff`* `commit_pending=true`
	Where:
	`none|hardpoweroff` – Type `none` for the system to take no action if the power policy is violated.Type `hardpoweroff` to immediately power off the system if the system power consumption violates the power policy.

Related Information

- Power Consumption Terminology and Properties
- Monitoring Power Allocations
- Getting Started With Oracle ILOM

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	• 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
- Monitoring Power Allocations

12 Performing Oracle ILOM Maintenance and Configuration Management Tasks

Description	Links
Refer to this section for information about performing firmware updates for upgradable system devices.	• Storing and Managing SP Firmware Images - As of Firmware Version 5.0 • Updating Oracle ILOM Firmware • Firmware Downgrade Package Restrictions
Refer to this section for information about resetting the power on the SP.	• Reset Power to Service Processor
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 • Managing Active and Standby SP Redundancy Roles (SPARC)
Refer to this section for instruction on how to back up, restore, or reset an Oracle ILOM SP configuration.	• Backing Up, Restoring, or Resetting the Oracle ILOM Configuration

Related Information

- Taking a Snapshot: Oracle ILOM SP State

Storing and Managing SP Firmware Images - As of Firmware Version 5.0

> **Note:**
>
> The ability to manage multiple SP firmware images in Oracle ILOM is supported on newer Oracle server platforms such as SPARC T7 and later platforms; as well as X86 X7 and later platforms. This functionality is *not* supported on SPARC M-Series platforms.

Oracle ILOM, as of firmware version 5.0, supports the ability to store and manage the following firmware images:

- **Current Firmware Image** – Refers to the firmware image that is currently running on the server SP.
- **Backup Firmware Image** – Refers to either: 1) the former firmware image that was previously installed on the server SP, or 2) a firmware image that was manually uploaded to the SP as the backup image.

Example: *Backup Image Behavior* — If the server SP is running firmware version 5.0.0 and is updated to 5.0.1. The current firmware image becomes version 5.0.1 and the backup firmware becomes version 5.0.0. If the backup image is manually updated to 5.0.2, the current firmware image remains at version 5.0.1 and the backup image becomes version 5.0.2.

SP Firmware Related Management Tasks - As of Firmware Version 5.0

As of Oracle ILOM firmware version 5.0, system administrators can choose to perform any of the following firmware management tasks:

- **Upload a Firmware Image for Immediate Installation** – Upload a firmware image from an external source to the SP for immediate installation. For instructions, see Updating Oracle ILOM Firmware.
- **Upload a Backup Image for Deferred Installation** – Upload a firmware image from an external source to the SP as a backup image that can be installed at a later time. For instructions, see Upload Firmware Backup Image for Deferred Installation.

> **Note:**
>
> Alternatively, system administrators (as of firmware version 5.0) can load a backup image using the Oracle ILOM REST API. For more information, see Upload Backup Image for Deferred Installation - Using REST API in .

- **Activate the Backup Image for Immediate Installation** – Activate the firmware backup image currently stored on the SP for immediate installation. For instructions, see Activate Firmware Backup Image for Immediate Installation.
- **View the Backup Image Properties** – View the firmware properties associated with the backup image such as upload date, version, and so. For instructions, see View Backup Firmware Image Properties

> **Note:**
>
> Alternatively, system administrators (as of firmware version 5.0) can view backup image properties using the Oracle ILOM REST API. For more information, see View Backup Image Properties - Using REST API.

Upload Firmware Backup Image for Deferred Installation

> **Note:**
>
> The ability to upload a backup firmware image is supported on newer Oracle server platforms such as SPARC T7 and later platforms; as well as X86 X7 and later platforms. This functionality is *not* supported on SPARC M-Series platforms.

Before You Begin

- The managed SP must have Oracle ILOM firmware version 5.0 or later installed.
- Oracle ILOM Admin (a) privileges to upload a backup firmware image.
- Verify that the managed server SP has network connectivity.
  For example, to verify that the server SP is connected to the network, use a remote web browser client or a remote CLI ssh client to log in to the server SP. For instruction, see Log In to the Oracle ILOM SP.
- 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.

- To upload a firmware backup image, perform the following steps using one of the Oracle ILOM interfaces:

Oracle ILOM Interface	Upload Backup Firmware Image (Deferred Installation)
Web	1. Click Maintenance > Firmware Update. 2. Click the button for Enter Update Mode, then click OK in the updateconfirmation dialog box to proceed. The Firmware Update page displays the properties associated with the current backup image. If a backup image does not exist on the SP, the property values "Not Available" appear. . 3. In the Firmware Update page, perform the following actions: 1. Select the checkbox for "Upload to the Backup Image". 2. Specify the firmware image to upload by either clicking Browse or URL. 3. Click the Upload button. Oracle ILOM stores the uploaded firmware image as the backup image and updates the properties associated with the backup image. **Note.** the backup image remains in a pending state until it is activated for installation. To active the backup image for immediate installation, see Activate Firmware Backup Image for Immediate Installation.

Oracle ILOM Interface	Upload Backup Firmware Image (Deferred Installation)

CLI	1. Type:
	`cd /SP/firmware/backupimage`
	2. To upload a backup firmware image to an SP from an external source, issue the `load` -source command followed by the path to the firmware image that you want to upload.
	For example:
	`load -source`
	`protocol://username:`
	`password@server_ip/<path_to_firmware.image>/<image.pkg>`
	Where the *protocol* can be: *http*, *https*, *ftp*, *tftp*, *sftp*, *scp*
	Upon successfully updating the backup image, a message similar to the following appears.
	`Oracle Integrated Lights Out Manager`
	`Version: #.#.#.#`
	`Copyright: © ####  Oracle and its affiliates. All rights reserved.`
	`…`
	`A new image is available in backupimage.`
	`HOSTNAME: ######`
	Note. The backup image remains in a pending state until it is activated for installation. To active the backup image for immediate installation, see Activate Firmware Backup Image for Immediate Installation

Related Information:

- Storing and Managing SP Firmware Images - As of Firmware Version 5.0

Activate Firmware Backup Image for Immediate Installation

> **Note:**
>
> The ability to activate a backup firmware image for installation is supported on newer Oracle server platforms such as SPARC T7 and later platforms; as well as X86 X7 and later platforms. This functionality is *not* supported on SPARC M-Series platforms.

Before You Begin

- Oracle ILOM Admin (a) privileges are required to activate the firmware backup image for installation.
- Verify that the managed server SP has network connectivity.
  For example, to verify that the server SP is connected to the network, use a remote web browser client or a remote CLI ssh client to log in to the server SP. For instruction, see Log In to the Oracle ILOM SP.
- To active the backup firmware image for immediate installation, perform the following steps using one of the Oracle ILOM interfaces:

Oracle ILOM Interface	Activate Backup Image (Immediate Installation)
Web	1. Click Maintenance > Firmware Update. 2. Click the button for Enter Update Mode, then click OK in the update confirmation dialog box to proceed. 3. In the Firmware Update page, perform the following actions: **Note.** The Firmware Update page displays the properties associated with the current backup firmware image. 1. Select the Backup Image button. 2. Click the Upload button. Oracle ILOM validates the firmware image and then displays options in the Firmware Verification page. **Note.** If the firmware update is to a previous firmware release, Oracle ILOM will validate the security level of the firmware image and determine whether to accept or prevent the update process. For more information, see Firmware Downgrade Package Restrictions 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 . **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 update 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 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 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. 8. To verify the current firmware version installed on the SP, click System Info > Firmware. **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. **Note.** After a backup image is activated as the current firmware image, the former firmware image installed on the SP becomes the backup image.

Oracle ILOM Interface	Activate Backup Image (Immediate Installation)

CLI	1. Type:
	`cd /SP/firmware`
	2. To activate the backup firmware image as the current firmware image, issue the `load` -source command followed by the path to the backup image.
	For example:
	`load -source /SP/firmware/backupimage`
	3. A series of prompts appear.
	4. 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 .
	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.
	5. 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.
	6. To verify the current firmware version installed, type:
	`show /system/firmware`
	Note. After a backup image is activated as the current firmware, the former firmware image installed on the SP becomes the backup image.

Related Information:

- Storing and Managing SP Firmware Images - As of Firmware Version 5.0

View Backup Firmware Image Properties

> **Note:**
>
> The ability to view backup firmware properties is supported on newer Oracle server platforms such as SPARC T7 and later platforms; as well as X86 X7 and later platforms. This functionality is *not* supported on SPARC M-Series platforms.

Before You Begin

- The managed SP must have Oracle ILOM firmware version 5.0 or later installed.
- Oracle ILOM Admin (a) privileges are required to view the backup firmware properties.

- To view the properties associated with the backup firmware image, perform the following steps using one of the Oracle ILOM interfaces:

Oracle ILOM Interface	View Backup Firmware Properties
Web	1. Click Maintenance > Firmware Update. 2. Click the button for Enter Update Mode, then click OK in the update confirmation dialog box to proceed. **Note.** The Firmware Update page displays the properties associated with the current backup Image. If a backup image does not exist on the SP, the property values "Not Available" appear.

CLI	1. Type:
	`show /SP/firmware/backupimage`
	Response Example:
	`/SP/firmware/backupimage`
	`    Targets:`
	
	`    Properties:`
	`        build = r129388`
	`        date = Fri Mar  8 09:28:46 PST 2019`
	`        load_uri = (Cannot show property)`
	`        upload_date = Fri Mar  8 09:31:50 2019`
	`        version = 5.0.0.0`
	
	`    Commands:`
	`        cd`
	`        load`
	`        set`
	`        show`

Related Information:

- Storing and Managing SP Firmware Images - As of Firmware Version 5.0

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

- Firmware Downgrade Package Restrictions
- Preserve Oracle ILOM Configuration
- Before You Begin the Firmware Update
- Update the Server SP Firmware Image
- Recover From a Network Failure During Firmware Update

Firmware Upgradable Devices

Oracle ILOM firmware images are available on the Oracle product download web site for Oracle x86 and SPARC servers:

For firmware download instructions, refer to Oracle ILOM Firmware Versions and Download Methods in *Oracle ILOM Feature Updates and Release Notes Firmware Release 5.0.x*.

Firmware Downgrade Package Restrictions

As of firmware release 5.0.0, Oracle ILOM verifies all firmware downgrade processes to prevent downgrades that might permit malicious actors exploiting known security vulnerabilities and gaining access to Oracle ILOM. For each downgrade request, Oracle ILOM prevents a downgrade to a less secure version by ensuring that the security level of the incoming firmware package meets or exceeds the security level of the currently installed package. If the incoming package matches or exceeds the security level checks, Oracle ILOM permits the downgrade process without restrictions. However, if the incoming package fails to meet the security level checks, Oracle ILOM displays a message indicating that the downgrade process has failed.

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. For additional information about updating the firmware to a prior firmware release, see Firmware Downgrade Package Restrictions.

Before You Begin the Firmware Update

Prior to updating the Oracle ILOM or individual device firmware, you should:

1. Verify that the managed server SP has network connectivity.

   For example, to verify that the server SP is connected to the network, use a remote web browser client or a remote CLI ssh client to log in to the server SP. For instruction, see Log In to the Oracle ILOM SP.

2. Identify the Oracle ILOM firmware version that is running on the managed server.

   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 5.0.x*.

4. Oracle ILOM Admin (a) privileges are required to update the firmware image.

5. Notify the SP 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.

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**

7. (Optional) Before updating firmware for monitored upgradable devices, suspend the Oracle ILOM Device Monitor feature if it is applicable for the server and if the feature is enabled. Monitored upgradable devices, such as RAID HBA or NVMe devices, can create FMA faults during a firmware update. After the individual device firmware updates have completed, re-enable device monitoring. For information on suspending and re-enabling device monitoring, see Setting Device Monitoring Configuration Properties.

Update the Server SP Firmware Image

System administrators can choose to start the firmware update process for upgradable devices from the web interface Actions panel, the Maintenance Firmware Update 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 firmware image have been met. See Before You Begin the Firmware Update.
- 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 image, perform the following steps using one of the Oracle ILOM interfaces:

Oracle ILOM Interface	Start and Run SP Firmware Update Procedure
Web	a. Click Maintenance > Firmware Update. b. Click the button for Enter Update Mode, then click OK in the update confirmation dialog box to proceed. **Note** – If the updated 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. c. In the Firmware Update page, perform these steps: i. Click the Upload Local File button. ii. Specify the firmware image to upload by either clicking Browse or URL. iii. Click the Upload button. Oracle ILOM validates the firmware image and then displays options in the Firmware Verification page. d. 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 . **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. e. Click Start to start the update process. f. Click OK to proceed through a series of prompts until the Update Status page appears. g. 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.

Oracle ILOM Interface	Start and Run SP Firmware Update Procedure
CLI	**a.** To load the Oracle ILOM firmware image using the CLI, issue the `load` -source command followed by the path to locate the firmware image you want to install. For example: `load -source` *`protocol://username:`* *`password@server_ip/<path_to_image>/<image.pkg>`* *Where* the *protocol* can be: *http*, *https*, *ftp*, *tftp*, *sftp*, *scp* A series of prompts appear. **b.** 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 . **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. **c.** 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:**
     Click System Information > Firmware.

     > **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

- File Transfer Methods
- Oracle ILOM Firmware Versions and Download Methods
- 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)
- Storing and Managing SP Firmware Images - As of Firmware Version 5.0

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.
3. Restart the firmware update process.

Reset Power to Service Processor

On occasion the server SP needs to be reset to complete an update or to clear an error state. The SP 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 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 the SP is reset.

System administrators can reset the server SP from the web interface or the CLI. For further SP reset instructions, see the following procedure.

Reset Power to Server SP

Before You Begin

- Host Control and Reset (r) role is required to reset a SP.
- 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, perform one of the following:

Oracle ILOM Interface	Reset Power to SP
Web	Click ILOM Administration > Maintenance > Reset SP, then click the Reset SP button.
CLI	Type: `reset /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	a. 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. b. 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	**a.** 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. **b.** 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	a. 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. b. Click ILOM Administration > Maintenance > Redundancy. c. View the Redundancy Status property. See SP Redundancy Status Descriptions.
CLI	a. 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. b. Type: `show /SP/redundancy` See SP Redundancy Status Descriptions.

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: **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.

Oracle ILOM Interface	Modify the roles of the active and standby SPs.
CLI	**a.** Type the following to navigate to the redundancy target: `cd /SP/redundancy` **b.** To set the failover action for the managed SP, type: `set initiate_failover_action=` *true*|*force* *true* **(Recommended Action)** — To gracefully negotiate the role change in a redundant SP system, set `true` as the Failover action. *force* **(Oracle Service Action)**— 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 server SP or use the backup file to install the configuration settings on other 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
- User Role Required for Backing Up or Restoring the Oracle ILOM Configuration
- Back Up the Oracle ILOM Configuration Settings
- Optionally Edit the Oracle ILOM Backup XML Configuration File
- Restore the Oracle ILOM Backup XML File
- Reset the Oracle ILOM Configuration to Factory Defaults

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 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.

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. At a minimum, the Admin (a) role is required to initiate the Restore operation.	• Privileges Granted by a User Profile Privileges Granted by a User Profile • Privileges Granted by Individual User Roles Privileges Granted by Individual User Roles • Configuring Local User Accounts
• Later releases of Oracle ILOM firmware version 3.2.6.x and all sequential 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.	

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. Upon initiating a Backup operation, all Oracle ILOM client sessions on the SP 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.

- 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. 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. 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 File Transfer Methods . 5. 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**. 6. Click Run to initiate the Backup operation. When the Backup operation is executing, client sessions to the Oracle ILOM SP are momentarily suspended. The sessions will resume to normal after the Backup operation is complete.

Oracle ILOM User Interface	Backing Up Oracle ILOM Configuration Settings to XML File

CLI	1. Navigate to the `config` CLI target, for example:
	`cd /SP/config`
	2. (Optional) To include fault data for all incidents in the backup operation, set the property value for `include_faultdata` to `true`. For instance:
	`set include_faultdata=true`
	The `include_faultdata` 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.
	3. To encrypt the backup configuration file, set the a value for the passphrase property, for example:
	`set passphrase=`*`value`*
	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**.
	4. To initiate the Backup operation, type the following command from within the `/SP/config`. For example:
	`set dump_uri=`*`transfer_method`*`://`
	`username``:`*`password`*`@`*`ipaddress_or_hostname`*`/`
	`directorypath``/`*`filename`*
	Where the *transfer method* can be:tftp, ftp, sftp, scp, http, or https
	For property descriptions of each file transfer method, see File Transfer Methods .
	For example:
	`set dump_uri=scp://adminuser:userpswd@1.2.3.4/Backup/`
	`Lab9/SP123.config`
	When the Backup operation is executing, client sessions to the Oracle ILOM SP 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
- Restore the Oracle ILOM Backup XML File
- Using Backup, Restore, and Reset Default Operations
- Managing Oracle ILOM Log Entries

Optionally Edit the Oracle ILOM Backup XML Configuration File

Advanced users can use the backup XML file to provision other Oracle server SPs 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:

   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.

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

   For example:

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

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

   - 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
- Restore the Oracle ILOM Backup XML File
- Using Backup, Restore, and Reset Default Operations

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 with the backed-up configuration data. Upon initiating a Restore operation, all Oracle ILOM client sessions to the restoring server SP 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 .
- 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.

- 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 File Transfer Methods . 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. **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 are momentarily suspended. The sessions will resume to normal after the Restore operation is complete.

Oracle ILOM User Interface	Restoring a Backup Copy of the Oracle ILOM Configuration Settings

CLI	1. Navigate to the `config` CLI target, for example:
	`cd /SP/config`
	2. (Optional) To restore previously backed up fault data in the xml configuration file, set the property value for `include_faultdata` to `true`. For instance:
	`set include_faultdata=true`
	The `include_faultdata` 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:
	set passphrase=*value*
	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 `/SP/config`. For example:
	set load_uri=*transfer_method*://*username*:*password*@*ipaddress_or_hostname*/*directorypath*/*filename*
	Where the *transfer method* can be:tftp, ftp, sftp, scp, http, or https.
	For property descriptions of each file transfer method, see File Transfer Methods .
	For example:
	set load_uri=scp://adminuser:userpswd@198.51.100.4/Backup/Lab9/SP123.config
	When the Restore operation is executing, client sessions to the Oracle ILOM SP are momentarily suspended. The sessions will resume to normal after the Restore operation is complete.

Related Information:

- Using Backup, Restore, and Reset Default Operations
- Restore the Oracle ILOM Backup XML File
- User Role Required for Backing Up or Restoring the Oracle ILOM Configuration

Reset the Oracle ILOM Configuration to Factory Defaults

System administrators can restore the current Oracle ILOM configuration settings on the SP 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, perform the following steps for one of the Oracle ILOM user interfaces listed.

Oracle ILOM Interface	Reset to Defaults Operation for SP
Web	1. Click ILOM Administration > Configuration Management > Reset Defaults. 2. Click the Reset Defaults list box to specify one of the following values: *None*, *All* or *Factory*. 3. Click the Reset Defaults button.
CLI	Type: `set /SP reset_to_defaults=`*`all`*`|`*`none`*`|`*`factory`*

Related Information:

- Reset Power to Service Processor

13

Maintaining x86 BIOS Configuration Parameters

Description	Links
Refer to this topic to identify ways you can manage the x86 BIOS configuration.	• BIOS Configuration Management
Refer to these topics for information about Oracle ILOM BIOS configuration features, terminology, and properties.	• Oracle ILOM: BIOS Configuration Features • Oracle ILOM: BIOS Terminology • Web and CLI: BIOS Properties
Refer to this section for information describing how to perform BIOS configuration tasks from Oracle ILOM.	• Performing BIOS Configuration Tasks From Oracle ILOM

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
- Oracle ILOM: BIOS Special Considerations
- Oracle ILOM: BIOS Terminology
- Web and CLI: BIOS Properties

> **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 .

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.

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.

Oracle ILOM Term	Description
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

- BIOS Web Navigation and CLI Targets BIOS Web Navigation and CLI Targets
- BIOS Web and CLI Properties BIOS Web and CLI Properties
- -force Option for CLI Commands: load and dump **-force** Option for CLI Commands: load and dump

Table 13-1 BIOS Web Navigation and CLI Targets

Web Navigation	CLI Targets
System Management > BIOS	`/System/BIOS` `/System/BIOS/Config`

Table 13-2 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.
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.

Table 13-2 (Cont.) BIOS Web and CLI Properties

Property Name	Type	Value(s)	Description
BIOS Configuration: Sync Status (config_sync_status=)	Read-only	OK|Reboot Required|Internal Error	**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 .

Table 13-2 (Cont.) BIOS Web and CLI Properties

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	**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.

Table 13-2 (Cont.) BIOS Web and CLI Properties

Property Name	Type	Value(s)	Description
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. **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.** **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 .

Table 13-2 (Cont.) BIOS Web and CLI Properties

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 13-3 `-force` Option for CLI Commands: `load` and `dump`

load_uri=-force *restore_option* **I** *transfer_method* **:II** *username:password* @ *ipaddress_or_hostname* **I** *directorypath* **I** *filename*
dump_uri=-force *transfer_method* **:II** *username:password* @ *ipaddress_or_hostname* **I** *directorypath* **I** *filename*
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)`.
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.

Table 13-3 (Cont.) `-force` Option for CLI Commands: `load` and `dump`

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
- View the BIOS Configuration Sync Status and Sync the Configuration Parameters
- Reset Factory Defaults for SP and Oracle ILOM BIOS
- Back Up the BIOS Configuration
- Restore BIOS Configuration

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 (`load_uri=`)	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 (`dump_uri=`)	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 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 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.

View the BIOS Configuration Sync Status and Sync the Configuration Parameters

Before You Begin

- Review the Requirements for BIOS Configuration Tasks.

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
- Reset Factory Defaults for SP and Oracle ILOM BIOS
- Back Up the BIOS Configuration
- Restore BIOS Configuration

Reset BIOS Configuration to Factory Defaults

Before You Begin

- Review the Requirements for BIOS Configuration Tasks.
- 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
- Reset Factory Defaults for SP and Oracle ILOM BIOS
- Back Up the BIOS Configuration
- Restore BIOS Configuration

Reset Factory Defaults for SP and Oracle ILOM BIOS

Before You Begin

- Review the Requirements for BIOS Configuration Tasks

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
- Reset BIOS Configuration to Factory Defaults
- Back Up the BIOS Configuration
- Restore BIOS Configuration

Back Up the BIOS Configuration

Before You Begin

- Review the Requirements for BIOS Configuration Tasks.
- 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
- -force Option for CLI Commands: load and dump
- View the BIOS Configuration Sync Status and Sync the Configuration Parameters
- Reset BIOS Configuration to Factory Defaults
- Reset Factory Defaults for SP and Oracle ILOM BIOS
- Restore BIOS Configuration

Restore BIOS Configuration

Before You Begin

- Review the Requirements for BIOS Configuration Tasks.
- 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.

> **Note:**
>
> Restore operation results are logged in the Oracle ILOM event log (`/SP/logs/event list`).

Related Information

- Web and CLI: BIOS Properties
- -force Option for CLI Commands: load and dump **-force** Option for CLI Commands: load and dump
- View the BIOS Configuration Sync Status and Sync the Configuration Parameters
- Reset BIOS Configuration to Factory Defaults
- Reset Factory Defaults for SP and Oracle ILOM BIOS
- Back Up the BIOS Configuration

Index