Oracle Integrated Lights Out Manager (ILOM) 3.1

Configuration and Maintenance Guide

Part No.: E24522-09
February 2014

Please
Recycle

Adobe PostScript

Contents

Using This Documentation

This configuration and maintenance guide provides web and CLI information about Oracle ILOM configuration and maintenance tasks.

Use this guide in conjunction with other guides in the Oracle ILOM 3.1 Documentation Library. This guide is intended for technicians, system administrators, and authorized Oracle service providers, and users who have experience managing system hardware.

Related Documentation

Documentation	Links
All Oracle products	http://www.oracle.com/documentation
Oracle Integrated Lights Out Manager (ILOM) 3.1 Documentation Library	http://www.oracle.com/pls/topic/lookup?ctx=ilom31

Documentation	Links
System management, single system management (SSM) security, and diagnostic documentation	http://www.oracle.com/technetwork/documentation/sys-mgmt-networking-190072.html
Oracle Hardware Management Pack 2.2	http://www.oracle.com/pls/topic/lookup?ctx=ohmp

Note: To locate Oracle ILOM 3.1 documentation that is specific to your server platform, see the Oracle ILOM section of the administration guide that is available for your server.

Documentation Feedback

Provide feedback on this documentation at:

http://www.oracle.com/goto/docfeedback

Product Downloads

Updates to the Oracle ILOM 3.1 firmware are available through standalone software updates that you can download from the My Oracle Support (MOS) web site for each Oracle server or blade chassis system. To download these software updates from the MOS web site, see the instructions that follow.

▼ Download Product Software and Firmware

1. **Go to** http://support.oracle.com**.**
2. **Sign in to My Oracle Support.**
3. **At the top of the page, click the Patches & Updates tab.**
4. **In the Patch Search panel, at the top of the Search tab, select Product or Family (Advanced).**

5. **In the Product Is list box, type a full or partial product name until a list of product matches appears in the list box, and then select the product name of interest.**

   Example product names: Sun Fire X4470 M2 Server or Sun Enterprise SPARC T5120.

6. **In the Release Is list box:**

   a. **Click the Down arrow in the Release Is list box to display a list of matching product folders.**

      A list of one or more product software releases appears.

   b. **Select the check box next to the software release of interest.**

      For example: `X4470 M2 SW 1.4` or `Sun SPARC Enterprise T5120`

7. **Click Search.**

   A Patch Search Results screen appears displaying a list of patch names and descriptions.

8. **In the Patch Search Results screen, select the Patch Name of interest.**

   For example: `X4470 M2 Server SW 1.4. ILOM and BIOS (Patch)` or `Firmware SPARC Enterprise T5120 Sun System Firmware 7.1.3.2`

9. **In the Patch Name selection, click one of the following actions:**
   - **Readme –** Opens the selected patch Readme file.
   - **Add to Plan –** Adds the selected patch to a new or existing plan.
   - **Download** – Downloads the selected patch.

Oracle ILOM 3.1 Firmware Version Numbering Scheme

Oracle ILOM 3.1 uses a firmware version numbering scheme that helps you to identify the firmware version you are running on your server or chassis monitoring module (CMM). This numbering scheme includes a five-field string, for example, `a.b.c.d.e`, where:

- `a` – Represents the major version of Oracle ILOM.
- `b` – Represents a minor version of Oracle ILOM.
- `c` – Represents the update version of Oracle ILOM.

- `d` – Represents a micro version of Oracle ILOM. Micro versions are managed per platform or group of platforms. See your platform product notes for details.
- `e` – Represents a nano version of Oracle ILOM. Nano versions are incremental iterations of a micro version.

For example, Oracle ILOM 3.1.2.1.a would designate:

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

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

Support and Accessibility

Description	Links

Access electronic support through My Oracle Support	`http://support.oracle.com`
	
	For hearing impaired:
	`http://www.oracle.com/accessibility/support.html`

Learn about Oracle's commitment to accessibility	`http://www.oracle.com/us/corporate/accessibility/index.html`

Setting Up a Management Connection to Oracle ILOM and Logging In

Description	Links
Refer to this section for information about supported management connection options to Oracle ILOM.	• "Establishing a Management Connection to Oracle ILOM" on page 1
Refer to this section for information about logging into Oracle ILOM, preconfigured user accounts, and supported operating systems and web browsers.	• "Logging In to Oracle ILOM Server SP or CMM" on page 18
Refer to this section for information on how to locate guidelines for enhancing Oracle ILOM security.	• "Configuring Oracle ILOM for Maximum Security" on page 25

Related Information

- Installation guide for Oracle servers or blade system CMM
- Administration guide for Oracle server
- *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide*

Establishing a Management Connection to Oracle ILOM

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

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

- "Choosing and Configuring a Management Connection to Oracle ILOM" on page 2
- "Management Services and Network Default Properties" on page 16

Choosing and Configuring a Management Connection to Oracle ILOM

Oracle ILOM supports the following management connections:

- "Dedicated Network Management Connection (Default)" on page 2
- "Sideband Network Management Connection" on page 4
- "Dedicated Local Management Connection" on page 7
- "Dedicated Interconnect SP Management Connection" on page 8

Dedicated Network Management Connection (Default)

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

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

▼ Configure a Dedicated Network Management Connection to Oracle ILOM

Before You Begin

- Review "Management Services and Network Default Properties" on page 16.
- The Management Port property in Oracle ILOM is, by default, set to route all management traffic through the physical network management port (NET MGT) on the managed device.

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

- To maintain the most reliable and secure environment for Oracle ILOM, the dedicated network management port on the server must always be connected to an internal trusted network or dedicated secure management/private network.
- The Management Port property for Oracle ILOM is configurable from the Oracle ILOM CLI and web interface. It is also configurable for x86 servers, from the BIOS Utility.

  If you modify the Management Port property from Oracle ILOM, you must log in using either the default `root` account or a user account with Admin (a) role privileges. For log in instructions, see "Log In to the Oracle ILOM SP or CMM" on page 19.

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

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

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

Note – When an active LAN connection is attached to the NET MGT port on the managed server or CMM chassis, Oracle ILOM automatically detects an IP address for the SP or CMM from the IP routing device on your network. For guidelines for determining the IP address assigned to the Oracle ILOM SP or CMM, see "Usage Guidelines for IP Network Management Address" on page 21.

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

User Interface	Step	Task: Verify or reset default management port property for SP or CMM
Oracle ILOM CLI	1:	Log in to the Oracle ILOM CLI and use the `show` command to view the network properties for the managed device, for example, type either: • **`show /SP/network`** • **`show /CMM/network`** For login instructions, see "Log In to the Oracle ILOM SP or CMM" on page 19.
	2:	Verify that the `/network` output displays the default Management Port property for the SP or CMM, for example: • SP output: `managementport=MGMT` • CMM output: `switchconf=port0`
	3:	If necessary, reset the default Management Port property for the SP or CMM. For SP, type: **`set /SP/network pendingmanagementport=MGMT commitpending=true`** For CMM, type: **`set /CMM/network pendingswitchconf=port0 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 or CMM" on page 19.
	2:	In the Network Settings page, verify that the Management Port list box for the SP is set to `MGMT` or the CMM Management Network Switch list box is set to `Port 0`. If necessary, reset the default Management Port property by selecting `MGMT` for SP or `Port0` for CMM, then click Save.
BIOS Setup Utility (only available for x86 servers)	1:	Access the BIOS Setup Utility on the managed x86 server, then in the BIOS Setup Utility dialog, click Advanced > IPMI 2.0 Configuration > Set LAN Configuration.
	2:	In the LAN Configuration menu, verify that the default Management Port property is set to `MGMT`. If necessary, reset the default Management Port property to `MGMT`, and then commit the change.

Related Information

- "Modifying Default Connectivity Configuration Properties" on page 92
- "Setting Up and Maintaining User Accounts" on page 27

Sideband Network Management Connection

For servers supporting sideband management, you can optionally connect to Oracle ILOM and manage the server remotely through the standard data port provided on the server chassis. Implementing a sideband management connection to Oracle ILOM eliminates the need to support two separate network connections for host and

management traffic. However, this approach could: (1) potentially decrease the connection performance to Oracle ILOM, and (2) potentially provide risks for transmitting Oracle ILOM traffic over an untrusted network.

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

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

- "Configure a Sideband Management Connection to Oracle ILOM" on page 5
- "Sideband Management Network Connectivity Considerations" on page 7

▼ Configure a Sideband Management Connection to Oracle ILOM

Before You Begin

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

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

- Review "Management Services and Network Default Properties" on page 16.
- To maintain the most reliable and secure environment for Oracle ILOM, the sideband management port on the server must always be connected to an internal trusted network or dedicated secure management or private network.
- The SP Management Port property for Oracle ILOM is configurable from the Oracle ILOM CLI and web interface. It is also configurable for x86 servers from the BIOS Setup Utility

  If you modify the Management Port property through Oracle ILOM, the following requirements apply:

  - A management connection to Oracle ILOM should already be established. For instructions, see either:

    - "Dedicated Network Management Connection (Default)" on page 2

    - "Dedicated Local Management Connection" on page 7

- You should have logged in to Oracle ILOM. For instructions, see "Logging In to Oracle ILOM Server SP or CMM" on page 18.
- 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/NET`*n*`commitpending=true`

     Where:

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

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

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

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

Related Information

- "Sideband Management Network Connectivity Considerations" on page 7
- "Usage Guidelines for IP Network Management Address" on page 21
- "Modifying Default Connectivity Configuration Properties" on page 92
- "Recommended Practice for Spanning Tree Configurations" on page 112
- "Setting Up and Maintaining User Accounts" on page 27
- "Assigning System Identification Information" on page 107

Sideband Management Network Connectivity Considerations

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

- In-chip connectivity between the server SP and the host operating system might not be supported by the on-board host Gigabit Ethernet controller. If this condition occurs, use a different port or route to transmit the traffic between the source and destination targets instead of using L2 bridging/switching.
- Server host power cycles might cause a brief interruption of network connectivity for server Gigabit Ethernet ports (`NET 0`, `1`, `2`, `3`) that are configured for sideband management. If this condition occurs, configure the adjacent switch/bridge ports as host ports.
- If the Ethernet data ports on the server are configured as switch ports and participate in the Spanning Tree Protocol (STP), you might experience longer outages due to spanning tree recalculations.

Dedicated Local Management Connection

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

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

▼ Configure a Dedicated Local Management Connection to Oracle ILOM

Before You Begin

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

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

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

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

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

Related Information

- "Management Services and Network Default Properties" on page 16
- "Modifying Default Connectivity Configuration Properties" on page 92
- "Assignable Oracle ILOM User Roles" on page 30
- "Serial Management Port Owner" on page 76
- "Assigning System Identification Information" on page 107

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.

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 Options for Local Interconnect" on page 9
- "Manually Configure the Local Interconnect" on page 9
- "Host OS Interconnect Guidelines for Manual Configuration" on page 12
- "Oracle ILOM SP Interconnect Properties" on page 15

Configuration Options for Local Interconnect

Local Interconnect Configuration Option	Description
Automatic Configuration (Recommended)	Oracle ILOM automates the configuration of the local interconnect management connection when you install the Oracle Hardware Management Pack 2.1.0 or later software. No configuration is necessary from Oracle ILOM in this case. **Note -** Automatic configuration of the local interconnect connection points require the default `Host Managed` (`hostmanaged`) setting in Oracle ILOM to be accepted (set to `True`), as well as the installation of the Oracle Hardware Management Pack 2.1.0 or later software on the server. For auto-configuration details, using the Oracle Hardware Management Pack, see the *Oracle Hardware Management Pack User's Guide*.
Manual Configuration (Advanced users)	If you are an advanced network administrator and prefer not to auto-configure the Ethernet USB connection points by installing the Oracle Hardware Management Pack, you can choose to manually configure the connection points on the internal Ethernet USB interface. For manual configuration details, see "Manually Configure the Local Interconnect" on page 9.

▼ 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

- Review "Configuration Options for Local Interconnect" on page 9.
- This manual procedure for configuring a local interconnect between the SP and host OS should be performed only by advanced users.
- This manual procedure provides guidelines for configuring the host OS internal connection point and detailed steps for optionally configuring the Oracle ILOM SP internal connection point.
- An established network or local serial management connection is required to the Oracle ILOM SP prior to modifying the default SP Local Host Interconnect properties in Oracle ILOM.

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

- The preconfigured Oracle ILOM `root` account or a customer-configured user account with Admin (`a`) role privileges is required to modify the SP Local Host Interconnect properties in Oracle ILOM.

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. **Verify that the server supports an internal Ethernet-over-USB interface.**

      To verify whether a server supports a local interconnnect management connection to Oracle ILOM, refer to the section describing Oracle ILOM supported features in the server administration guide.

   b. **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*.

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

      For guidelines, see "Host OS Interconnect Guidelines for Manual Configuration" on page 12.

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

   a. **Review** "Oracle ILOM SP Interconnect Properties" on page 15**.**

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

      For log in instructions see, "Logging In to Oracle ILOM Server SP or CMM" on page 18.

   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	Step:
Web-browser	1. In the Oracle ILOM SP web interface, click ILOM Administration > Connectivity. 2. Scroll down the page to the Local Host Interconnect section and click Configure. 3. In the Configure USB Ethernet Parameters dialog, clear the check box for Host Managed, enable the check box for State, and only if necessary, modify the local non-routable IPv4 address or netmask addresses provided for the SP, then click Save. **Note**. You do not need to modify the preconfigured IP address or netmask address assigned to the Oracle ILOM SP, unless a conflict with these parameters exists in your network.
CLI shell	1. Navigate to the `/network/interconnect` working directory on the managed server. **For example:** From SP CLI, type: **`cd /SP/network/interconnect`** From CMM CLI, type: **`cd /Servers/Blades/BL`*n*`/network/interconnect`** 2. To disable the `hostmanaged` property and to set the Local Host Interconnect state to `true`, type the following: **`set hostmanaged=disabled`** **`set state=true`** **Note**. You do not need to modify the preconfigured non-routable IP address and netmask address assigned to the Oracle ILOM SP, unless a conflict with these parameters exists in your network. 3. To modify the local non-routable IPv4 address or netmask address provided for the SP, type the following: **`set pendingipaddress=`***specify_new_address* **`set pendingipnetmask=`***specify_new_address* **`set commitpending=true`**

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

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

     Expected results for:

     Web browser connection – The Oracle ILOM Login page appears.

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

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

     For instructions, see "Test IPv4 and IPv6 Connectivity" on page 113.

Related Information

- "Host OS Interconnect Guidelines for Manual Configuration" on page 12
- "Oracle ILOM SP Interconnect Properties" on page 15
- "Logging In to Oracle ILOM Server SP or CMM" on page 18
- *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide*, Understanding the LAN Interconnect Interface
- 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: Host OS Interconnect Manual Configuration Guidelines

Operating System	Manual Host OS Interconnect Guidelines
Windows Server 2008	After Microsoft Windows discovers the internal Ethernet-over-USB interface on the managed server, a message might appear prompting you to identify a device driver for the Ethernet-over-USB interface. Since no driver is actually required, identifying the `.inf` file, which is extractable from the Oracle Hardware Management Pack software distribution, should satisfy the communication stack for the Ethernet-over-USB interface. The software distribution for the Oracle Hardware Management Pack 2.1.0 or later is available for download from the Oracle software product download page. For information about extracting the `.inf` file from the Oracle Server Hardware Management Pack, refer to the *Oracle Server Hardware Management Pack User's Guide*. For additional details that describe how to configure IP network parameters in Windows Server 2008, see the Microsoft Windows Operating System documentation or refer to the following Microsoft Tech Net site: `http://technet.microsoft.com/en-us/library/cc754203%28WS.10%29.aspx`

Linux	Most supported Linux operating system installations on a managed server include the installation of the device driver for the Ethernet-over-USB interface.
	The Ethernet-over-USB interface is, typically, automatically discovered by the Linux operating system and presented in the system as `usb0`. However, the name presented for this interface might vary for a given Linux software distribution.
	The following command-line instructions demonstrate how to configure network parameters for the host OS interconnect connection corresponding to `usb0`:
	`\>lsusb usb0`
	`\> ifconfig usb0 169.254.182.77`
	`\> ifconfig usb0 netmask 255.255.255.0`
	`\> ifconfig usb0 broadcast 169.254.182.255`
	`\> ifconfig usb0`
	`\> ip addr show usb0`
	Note - Rather than issuing individual `ifconfig` commands, you can script the network parameter configuration. However, the exact network script for configuring network parameters can vary among Linux software distributions. Therefore, you should refer to the network script examples that are typically provided with each Linux software distribution.
	For additional details about how to configure IP network parameters using a Linux operating system, refer to the Linux operating system documentation.

TABLE: Host OS Interconnect Manual Configuration Guidelines *(Continued)*

Operating System	Manual Host OS Interconnect Guidelines

Solaris	Most Oracle Solaris Operating System installations on a managed server include the device driver for the Ethernet-over-USB interface. If the device driver for this interface was not provided, you can extract this driver from the Oracle Hardware Management Pack 2.1.0 or later software distribution.
	For information about extracting the Solaris-specific OS driver from the management pack, refer to the *Oracle Hardware Management Pack User's Guide*.
	The Ethernet-over-USB interface is, typically, automatically discovered by the Oracle Solaris Operating System and presented in the system as `usbecm0`. However, the name presented for this interface might vary among Oracle Solaris software distributions.
	The following command-line instructions demonstrate how to configure network parameters for the host OS interconnect connection corresponding to `usbecm0`.
	• Type one of the following commands to `plumb` the IP interface or `unplumb` the IP interface:
	`ifconfig usbecm0 plumb`
	`ifconfig usbecm0 unplumb`
	• Type the following commands to set the address information:
	`ifconfig usbecm0 netmask 255.255.255.0 broadcast 169.254.182.255 169.254.182.77`
	• To set up the interface, type:
	`ifconfig usbecm0 up`
	• To bring the interface down, type:
	`ifconfig usbecm0 down`
	• To show the active interfaces, type:
	`ifconfig -a`
	• To test connectivity, ping the Oracle Solaris host or the SP internal USB Ethernet device.
	`ping` *<IPv4 address of Oracle Solaris host>*
	`ping` *<IPv4 address of SP Ethernet-over-USB interface>*
	Note - Rather than performing the `ifconfig` steps, you can script the network parameter configuration. However, the exact network script for configuring network parameters can vary among each Oracle Solaris software distribution. Therefore, you should refer to the network script examples that are typically provided with each Oracle Solaris software distribution.
	For more information about how to configure a static IP address for a hardware device using the Oracle Solaris Operating System, refer to the Oracle Solaris Operating System documentation.

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: Oracle ILOM SP Interconnect Properties

Property	Default Value	Description
Host Managed (`hostmanaged=`*true*|*false*)	Enabled (`true`)	The Host Managed property, by default, arrives ready for the Oracle Hardware Management Pack software to auto-configure the local interconnect management connection between the host OS and the Oracle ILOM SP. To prevent the Oracle Hardware Management Pack software from auto-configuring the local interconnect connection or to manually configure the connection points between the host OS and the Oracle ILOM SP, the value for the Host Managed property must be set to disabled (`false`). **Note**. To prevent the use of the Ethernet-over-USB interface, both the Host Managed property and the Local Host Interconnect state property must be disabled (`false`) in Oracle ILOM.
State (`state=`*disabled*|*enabled*)	`Disabled`	The state for the Local Host Interconnect property in Oracle ILOM is set, by default, to disabled. 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.
IP Address (`pendingipaddress=`)	`169.254.182.7`	Oracle ILOM, by default, provides a preconfigured non-routable IPv4 address for the Oracle ILOM SP Ethernet-over-USB connection point. You typically will not need to change the preconfigured IP address (169.254.182.76), unless a conflict with this address exists in your network.
Netmask Address (`pendingipnetmask=`)	`255.255.255.0`	Oracle ILOM, by default, provides a preconfigured IPv4 Netmask Address for the Oracle ILOM SP Ethernet-over-USB connection point. 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.
Save (`commitpending=`*true*|*false*)		Any modifications made to IP Address or Netmask Address for the Oracle ILOM SP Ethernet-over-USB connection point are considered pending until the changes are committed in the CLI or saved in the web interface.

TABLE: Oracle ILOM SP Interconnect Properties *(Continued)*

Property	Default Value	Description
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.
Host MAC Address (`hostmacaddress=`)	Read-only	The read-only property for the Host MAC Address displays the MAC address that is assigned to the managed server and it also represents how most operating systems recognize the internal Ethernet-over-USB interface.
Connection Type	Read-only	This read-only Connection Type property indicates the connection type of the internal USB Ethernet.
CLI `help` command		For additional information about configurable or non-configurable properties appearing under the `/network/interconnect` CLI target, you can type the `help` command followed by the property name. **Syntax:** **`help`** */SP|CMM***`/network/interconnect`** *property_name* **Example:** **`help /SP/network/interconnect hostmanaged`**

Management Services and Network Default Properties

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

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

- TABLE: Management Services Enabled by Default on page 17
- TABLE: Network Connectivity Properties Enabled by Default on page 18

TABLE: Management Services Enabled by Default

Management Access	Default Properties	Service Port	To modify configurable properties, see;
Web Server: Mode	• Redirect HTTP Connection to HTTPS	80	TABLE: Web Server Configuration Properties on page 79
Web Server: State	• HTTPS, Enabled	443	TABLE: Web Server Configuration Properties on page 79
Web Server: SSL	• SSLv3 and TLSv1 Enabled • Default SSL certificate • Default SSL self-signing private key	-	TABLE: SSL Certificate and Private Key Configuration Properties for HTTPS Web Server on page 82
IPMI: State	• Enabled	623	TABLE: IPMI Service Configuration Properties on page 89
SNMP: State	• SNMPv3, Enabled	161	TABLE: SNMP Configuration Properties on page 84 **Note -** For a higher level of security, Oracle ILOM IPMI clients should always support and operate in IPMI 2.0 mode.
WS-MAN: Mode	• HTTP, Enabled	8889	TABLE: WS-Man Web Service Configuration Properties on page 91
Single Sign On	• Enabled	11626	"Single Sign-On Service (Enabled by Default)" on page 32
Secure Shell (SSH)	• Enabled • RSA and DSA Key Generation	22	TABLE: SSH Server Configuration Properties on page 88
Remote KVMS Redirection (video, keyboard, mouse, and storage)	• Enabled	5120-5123, 5555, 5556, 7578, 7579	"Using Remote KVMS Consoles for Host Server Redirection" on page 115
Service tag*	• Enabled	6481	To modify the service tag property, type: **`set /SP/services/servicetag state=`** *enabled | disabled*

* An Oracle discovery protocol that identifies servers and provides intergration to Oracle service solutions.

Note – For a complete list of default network ports used by Oracle ILOM, see "Default Network Ports Used by Oracle ILOM" on page 76.

TABLE: Network Connectivity Properties Enabled by Default

Network Connectivity Property	Default Value	To modify configurable properties, see:
Network: State	• Enabled	TABLE: Network Connectivity Configuration Properties on page 93
IPv4: Mode	• DHCP, enabled	
IPv6: State	• Enabled	TABLE: Network Connectivity Configuration Properties on page 93
IPv6: Mode	• Auto-Config, Stateless	
Management Port:	• Dedicated Network Management (MGMT)	TABLE: Network Connectivity Configuration Properties on page 93
Local Host Interconnect	• Host Utilities Managed: Enabled • State: Disabled	"Dedicated Interconnect SP Management Connection" on page 8
DNS	• Auto DNS via DHCP, Enabled	TABLE: DNS Configuration Properties on page 101
Serial Port	• Owner: Service Processor • Baud Rate: 9600 • Host Flow Control: None	TABLE: Serial Port Configuration Properties on page 103
User Authentication*	• Root user account: root • Root password: `changeme` • Permitted local accounts: Up to 10 customer-configurable user accounts • Single Sign On: Enabled for remote KVMS and CMM blade navigation (drill-down).	"Managing User Credentials" on page 28

* The property states for LDAP, RADIUS, and Active Directory are, by default, disabled.

Logging In to Oracle ILOM Server SP or CMM

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

- "Log In to the Oracle ILOM SP or CMM" on page 19
- "Usage Guidelines for IP Network Management Address" on page 21
- "Preconfigured User Accounts Enabled by Default" on page 22

- "Supported Operating System Web Browsers" on page 24

▼ Log In to the Oracle ILOM SP or CMM

Before You Begin

- An established local or network management connection to Oracle ILOM is required.

  For instructions, see "Choosing and Configuring a Management Connection to Oracle ILOM" on page 2.

- The preconfigured Oracle ILOM `root` account or a customer-configured user account is required to log in to Oracle ILOM.

  For information about the preconfigured `root` account, see "Preconfigured User Accounts Enabled by Default" on page 22. For information about how to create user accounts in Oracle ILOM, see "Managing User Credentials" on page 28.

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	1. Type **`http://`***ILOM_SP_or_CMM_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" on page 21. 2. 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	1. To establish an SSH session to the Oracle ILOM CLI, open a terminal window. 2. To log in to Oracle ILOM using the default `root` account, type: $ **`ssh root@`***ILOM_SP_or_CMM_ipaddress* Oracle ILOM prompts you for the `root` password. 3. 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" on page 107
- "Default Timeout for CLI and Web Sessions" on page 75
- "Modifying Default Management Access Configuration Properties" on page 78
- "Displaying Banner Messages at Log-In" on page 75
- "Setting Up and Maintaining User Accounts" on page 27
- "Password Recovery for root Account" on page 35
- "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1
- "Using Remote KVMS Consoles for Host Server Redirection" on page 115
- *Oracle ILOM 3.1 User's Guide,* "Collecting System Information, Monitoring Health Status, and Initiating Host Management" on page 33

- *Oracle ILOM 3.1 User's Guide*, "CLI Reference For Mapping Management Tasks to CLI Targets" on page 124
- "Performing Firmware Updates" on page 190

Usage Guidelines for IP Network Management Address

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

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

To determine:	Guidelines
IP address assigned to Oracle ILOM	To determine the assigned IP address, perform these steps. 1. Establish a local serial management (SER MGT) connection to the ILOM SP or CMM. 2. Log in to Oracle ILOM 3. Use the `show` command to view the IP network properties under: `/SP/network` for the current IPv4 address assigned to Oracle ILOM. `/SP/networkipv6` 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.

TABLE: IP Address Identification, IPv6 Accepted Syntax, Non-supporting IPv6 servers *(Continued)*

To determine:	Guidelines	
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 enclose*d 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 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: 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*, 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 or CMM, you should either: • Modify the default `root` password (`changeme`) provided on each Oracle ILOM service processor (SP) or chassis monitoring module (CMM). - or - • Delete the preconfigured `root` account provided on the Oracle ILOM SP and Oracle ILOM CMM. Prior to removing the preconfigured `root` account, you must replace the `root` account with a customer-configurable local user account or a directory service such as LDAP or Active Directory. **Note.** When the `root` account password is set to `changeme` (default password), a warning message appears in the CLI upon logging in and a warning message appears in the top portion of the web interface page.	"Managing User Credentials" on page 28

TABLE: Local User Accounts Enabled by Default *(Continued)*

Preconfigured User Account	Default Login Properties	Description	To modify, see:
default	• `Username: default` • `Password: defaultpassword`	The preconfigured `default` user account provided in Oracle ILOM is limited to password recovery. **Local serial console use only** – The preconfigured `default` user account is available for use through a local serial connection only. Also, you must be able to prove physical presence at the server or CMM. **Usage Scenario** – If you delete the `root` account in Oracle ILOM prior to replacing the root account with a customer-configurable account, you can use the `default` account to log in to Oracle and use the normal Oracle ILOM commands to create a new account. **Related Information**: • TABLE: Recover Preconfigured root Account or root Account Password (CLI only) on page 36 • (Physical Presence) "Assigning System Identification Information" on page 107	"Password Recovery for root Account" on page 35

* Oracle ILOM web interface, CLI shell, local serial console, and IPMI.

Supported Operating System Web Browsers

Oracle ILOM supports the following operating system web browsers.

Note – For a list of operating systems supported by the managed server, refer to the server administration guide or product notes.

TABLE: Supported Operating System Web Browsers

Operating System	Web Browser
Oracle Solaris 10	• Mozilla 1.4 and 1.7 • Firefox 3.6.x and 6
Linux (Oracle, Red Hat, SuSE, Ubuntu 10.10)	• Firefox 3.6.x and 6
Microsoft Windows (XP Service Pack 2, Windows 7)	• Internet Explorer 7.x, 8.x (for Windows XP Service Pack 2), and 9 (for Windows 7) • Firefox 3.6.x and 6
Macintosh (OSX v10.6 and later)	• Firefox 3.6.x and 6 • Safari – all

Configuring Oracle ILOM for Maximum Security

All configurable properties in Oracle ILOM can be optionally disabled or enabled to make the Oracle ILOM management environment more secure. For further details about enhancing security in Oracle ILOM, refer to the security guidelines described in the *Oracle ILOM 3.1 Security Guide*.

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 removing preconfigured `root` account and password.	• "Managing User Credentials" on page 28
Refer to this section for requirements and instructions for configuring local user accounts in Oracle ILOM.	• "Configuring Local User Accounts" on page 37
Refer to this section for requirements and instructions for configuring Oracle ILOM as an Active Directory client.	• "Configuring Active Directory" on page 40
Refer to these sections for requirements and instructions for configuring Oracle ILOM as an LDAP/SSL client or LDAP client.	• "Configuring LDAP/SSL" on page 52 • "Configuring LDAP" on page 62
Refer to this section for requirements and instructions for configuring Oracle ILOM as a RADIUS client.	• "Configuring RADIUS" on page 66

Related Information

- *Oracle ILOM 3.1 Protocol Management Reference Guide*, "Manage User Accounts Using SNMP" on page 33
- *Oracle ILOM 3.1 Security Guide*, Oracle ILOM security at deployment
- "Preconfigured User Accounts Enabled by Default" on page 22

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

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

TABLE: User Authentication Configuration Options

Option	Features and Considerations	
Local User Account Authentication	• Up to 10 configurable user accounts stored locally in Oracle ILOM. • Two preconfigured user accounts are shipped for quick deployment and maintenance: `root` user account and `default` user account (see "Preconfigured User Accounts Enabled by Default" on page 22). • Configurable user role privileges granting either read-only or read and write access to discrete Oracle ILOM features (see "Assignable Oracle ILOM User Roles" on page 30). • Secure user authentication and authorization for local and remote management. • Oracle ILOM user credentials are maintained separately for each SP and CMM. For additional information about configuring local user accounts in Oracle ILOM, see "Configuring Local User Accounts" on page 37.	
Authentication Directory Service	• Provides users access to Oracle ILOM beyond 10 local user accounts. • Enables system administrators to centrally create and maintain user credentials for all Oracle ILOM instances (all managed server SPs and CMMs in local network environment). • Enables authenticated Oracle ILOM users to have access to all Oracle ILOM instances. • Enables system administrators to configure user authentication rules for using features within Oracle ILOM.	
	Supported Authentication Services	
	Active Directory	Active Directory is a distributed service that is provided with Microsoft Windows Server operating systems. The Active Directory service is secure by default. For additional information about configuring Oracle ILOM to use the Active Directory authentication service, see "Configuring Active Directory" on page 40.
	LDAP/SSL	The LDAP/SSL authentication service is secure by default. It supports an optional strict certification mode that requires the use of a security certificate. For information about configuring Oracle ILOM as an LDAP/SSL client, see "Configuring LDAP/SSL" on page 52.
	LDAP	The LDAP (v2) authentication service is less secure than LDAP/SSL. Configure this service only if you understand and accept the security limitations. For additional information about configuring Oracle ILOM as a LDAP client, see "Configuring LDAP" on page 62.

TABLE: User Authentication Configuration Options *(Continued)*

Option	Features and Considerations	
	RADIUS	Remote Authentication Dial In User Service (RADIUS) is a networking protocol that uses a client-server model to provide user authentication and authorization. For additional information about configuring Oracle ILOM to use the RADIUS authentication service, see "Configuring RADIUS" on page 66.

Assignable Oracle ILOM User Roles

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

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

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

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

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

- TABLE: Privileges Granted by a User Profile on page 31
- TABLE: Privileges Granted by Individual User Roles on page 32

TABLE: Privileges Granted by a User Profile

Web Property	CLI Property	Privileges Granted by Profile
Administrator	administrator	The Administrator (`administrator`) profile is predefined with the following user roles. • Admin (a) • User Management (u) • Console (c) • Reset and Host Control (r) • Read-Only (o) For a description of privileges granted by each user role, see TABLE: Privileges Granted by Individual User Roles on page 32.
Operator	operator	The Operator (`operator`) profile is predefined with the following user roles: • Console (c) • Reset and Host Control (r) • Read-Only (o) For a description of privileges granted by each user role, see TABLE: Privileges Granted by Individual User Roles on page 32.
Advanced Roles	*a* | *u* | *c* | *r* | *o* | *s*	The Advanced Roles profile option is user-configurable from the web interface only. The Advanced Roles profile option enables system administrators to assign any of the following six user roles to a single user account: • Admin (a) • User Management (u) • Console (c) • Reset and Host Control (r) • Read-Only (o) • Service (s) **Note -** The same six user roles (*a* | *u* | *c* | *r* | *o* | *s*) are individually assignable to a single user account from the CLI. For a description of privileges granted by each user role, see TABLE: Privileges Granted by Individual User Roles on page 32.

TABLE: 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 Console, and launch and use Oracle ILOM Storage Redirection CLI.
Reset and Host Control (r)	The Reset and Host Control (r) user role, when enabled, grants read and write permissions to perform these host management functions: host boot device control, run and configure diagnostics utilities, reset SP, reset CMM, sub-component service actions, fault management actions, SPARC TPM management actions, and SNMP MIB download operation.
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 and session time-out properties assigned to the individual user account.
Service (s)	The Service (s) user role, when enabled, grants read and write permissions to assist Oracle service engineers if on-site service is required.
a|u|c|r|o	A combination of all these users roles (aucro), when enabled, grants read and write permissions to perform backup and restore configuration functions in Oracle ILOM.

Single Sign-On Service (Enabled by Default)

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

- Oracle ILOM SP web interface authenticated users to launch the KVMS applications (Oracle ILOM Remote Console or Oracle ILOM Storage CLI Redirection) without requiring users to re-enter their passwords.
- Oracle ILOM CMM authenticated users to navigate to individual managed blade servers installed in the chassis, without requiring users to re-enter their passwords. For more information about managing blade servers from the CMM web interface or CLI, refer to the *Oracle ILOM 3.1 User's Guide,* "Managing Blade Servers From the CMM CLI" on page 26.

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

User Interface Configurable Target:

- **CLI**: */SP|CMM/services/*
- **Web**: ILOM Administration > User Management > User Accounts > Single Sign On
- **User Role:** Admin (a) (required for property modification)

Property	Default Value	Description
Single Sign On (/sso state=)	Enabled	*Enabled* | *Disabled* **CLI SSO State Syntax:** **set /***SP*|*CMM***/services/sso state=***enabled*|*disabled*

Maximum Number of User Sessions Supported

Oracle ILOM supports a maximum of 10 active user sessions per managed server SP or CMM. Some SPARC systems are limited to a maximum of 5 active user sessions per managed server SP.

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

Viewable User Authenticated Sessions per Managed Device

System administrators can identify a list of users who are actively logged in to an Oracle ILOM SP or CMM using the CLI or web interface. To view a list of user sessions for a single SP or CMM instance, see the following table.

User Interface Configurable Target:

- **CLI**: /*SP*|*CMM*/services/
- **Web**: ILOM Administration > User Management > Active Sessions
- **User Role:** Administrator (administrator) profile (aucro)

Property	Description
Active Sessions (sessions)	The Active Sessions information, for a single SP or CMM, lists the authenticated user sessions currently logged in to Oracle ILOM. **CLI Active Sessions Syntax**: • **show /***SP*|*CMM***/sessions** • **show /***SP*|*CMM***/sessions***n*

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.

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: Adding or Removing Public SSH Key File per Local User Account

User Interface Configurable Target:

- **CLI**: /*SP*|*CMM*/services/
- **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 TABLE: File Transfer Methods on page 37.

TABLE: Adding or Removing Public SSH Key File per Local User Account *(Continued)*

User Interface Configurable Target:

- **CLI**: */SP|CMM/services/*
- **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
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@1.2.3.4/keys/sshkey_1.pub
Delete SSH Key (clear action=true)	**CLI Delete SSH Key Syntax**: **set /***SP|CMM***/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 TABLE: View, Modify, or Remove User Account on page 39.

Password Recovery for 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: 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 the 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
	• "Configure a Dedicated Local Management Connection to Oracle ILOM" on page 7
	• (Physical Presence) "Assigning System Identification Information" on page 107
	• TABLE: Create User Account and Assign User Roles on page 38
	• TABLE: View, Modify, or Remove User Account on page 39

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: 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.
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:

- TABLE: Create User Account and Assign User Roles on page 38
- TABLE: View, Modify, or Remove User Account on page 39

TABLE: Create User Account and Assign User Roles

User Interface Configurable Target:

- **CLI**: /*SP*|*CMM*/users/
- **Web**: ILOM Administration > User Management > User Accounts
- **User Role:** User Management (u) (required for all property modifications)

Property	Description
Users > Add (*user_name* password= role =)	*user_name* |Password=|Role=*administrator* |*operator*|*advanced* (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. **CLI Create User Syntax**: **create /***SP*|*CMM***/users/***user_name_for_account* **password=** *password_for_account* **role=***administrator*|*operator*|*a*|*u*|*c*|r|o|s **Example Syntax:** create /SP/users user5 password=administrator role=aucr **Note**. When adding a user account through the CLI, it is unnecessary to provide a property value for a role or password. The role will default to Read-Only (o), and the CLI will prompt you to provide and confirm a password.
Save	**Web interface** – To apply changes made to properties within the Add User dialog, you must click Save.
	Related Information: • TABLE: Privileges Granted by a User Profile on page 31 • TABLE: View, Modify, or Remove User Account on page 39 • TABLE: Local User Accounts Enabled by Default on page 23 • TABLE: Recover Preconfigured root Account or root Account Password (CLI only) on page 36 • "CLI Authentication Using Local User SSH Key" on page 34

TABLE: View, Modify, or Remove User Account

User Interface Configurable Target:

- **CLI**: /*SP*|*CMM*/users/
- **Web**: ILOM Administration > User Management > User Accounts
- **User Role:** User Management (u) (required for all property modifications)

Property	Description
Users (/users)	View local user accounts configured in Oracle ILOM. **CLI View Users Syntax**: **show /***SP*|*CMM***/users** **Example syntax:** show /SP/users
Users > Edit (/*user_name* password= role=)	Password=*user_configurable*|role=*administrator* |*operator*|*advanced* (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 root user. **Web interface** – Click Save to apply the changes made within the Edit User dialog. **CLI Edit User Account Syntax**: **set /***SP*|*CMM***/users** *user_name* **password=***assign_new_password* **role=** *administrator*|*operator*|*a*|*u*|*c*|r|o|s **Example Syntax**: set /SP/users user5 password=administrator role=auco
Users > Delete (/*user_name*)	Specify the name of the user account to delete. When prompted, confirm the action. **CLI Delete User Account Syntax:** **delete /***SP*|*CMM***/users**/*user_name* **Example Syntax:** delete /SP/users/user5
	Related Information: • "Security Action: Change Default root Account Password" on page 35 • TABLE: Privileges Granted by a User Profile on page 31 • TABLE: Create User Account and Assign User Roles on page 38 • TABLE: Recover Preconfigured root Account or root Account Password (CLI only) on page 36

Configuring Active Directory

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

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

- TABLE: Enabling Active Directory Authentication on page 41
- TABLE: Uploading or Removing an Active Directory Certificate File on page 45
- TABLE: Optionally Configuring Active Directory Groups on page 46
- TABLE: Configuring Active Directory User Domains on page 49
- TABLE: Optionally Configuring Active Directory Alternate Servers on page 50
- TABLE: Optionally Editing DNS Locator Queries on page 51
- TABLE: Guidelines for Troubleshooting Active Directory Authentication on page 52

TABLE: Enabling Active Directory Authentication

User Interface Configurable Target:

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

Property	Default Value	Description
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|CMM***/clients/activedirectory/ state=***disabled|enabled
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|CMM***/clients/activedirectory/ defaultrole=** *administrator|operator|a|u|c|r|o|s|none* **Related Information:** • TABLE: Privileges Granted by a User Profile on page 31 • TABLE: Privileges Granted by a User Profile on page 31 • TABLE: Optionally Configuring Active Directory Groups on page 46

TABLE: Enabling Active Directory Authentication *(Continued)*

User Interface Configurable Target:

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

Property	Default Value	Description
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*|*CMM***/clients/activedirectory/ address=** *active_directory_server ip_address*|*active_directory_server_dns_host_name* **Related Information:** • TABLE: DNS Configuration Properties on page 101
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*|*CMM***/clients/activedirectory/ port=***number*
Timeout (timeout=)	4 seconds	*4*	*user-specified* The Timeout property designates the number of seconds to wait for an individual transaction to complete. The value does not represent the total time for all transactions to complete since the number of transactions can differ depending on the configuration. The Timeout property is set to 4 seconds by default. If necessary, adjust this property value as needed to fine tune the response time for when the Active Directory server is unreachable or not responding. **CLI Timeout Syntax**: **set /***SP*|*CMM***/clients/activedirectory/ timeout=** *number_of_seconds*

TABLE: Enabling Active Directory Authentication *(Continued)*

User Interface Configurable Target:

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

Property	Default Value	Description
Strict Certificate Mode (strictcertmode=)	Disabled	*Disabled* | *Enabled* When the Strict Certificate Mode property is enabled, Oracle ILOM fully verifies the digital signatures in the Active Directory certificate at the time of authentication. When the Strict Certificate Mode property is disabled, Oracle ILOM provides limited validation of the server certificate at the time of authentication over a secure channel. **Caution -** The Active Directory server certificate must be loaded prior to enabling the Strict Certificate Mode property. **CLI Strict Certificate Mode Syntax**: **set /***SP*|*CMM***/clients/activedirectory/ strictcertmode=** *disabled*|*enabled* **Related Information**: • TABLE: Uploading or Removing an Active Directory Certificate File on page 45
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*|*CMM***/clients/activedirectory/ dnslocatorqueries/1=** *disabled*|*enabled* **Related Information**: • TABLE: Optionally Editing DNS Locator Queries on page 51
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*|*CMM***/clients/activedirectory/ expsearchmode=** *disabled*|*enabled*

TABLE: Enabling Active Directory Authentication *(Continued)*

User Interface Configurable Target:

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

Property	Default Value	Description
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 Certificate Mode Configuration Syntax**: **set /***SP*|*CMM***/clients/activedirectory/ strictcredentialerrormode=***disabled*|*enabled* **Related Information**: • TABLE: Uploading or Removing an Active Directory Certificate File on page 45
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*|*CMM***/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: Uploading or Removing an Active Directory Certificate File

User Interface Configurable Target:

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

Property	Default Value	Description
Certificate File Status (certstatus=)	Read-only	*Certificate present* | *Certificate not present* The Certificate File Status property indicates whether an Active Directory certificate has been uploaded to Oracle ILOM. **Caution -** The Active Directory certificate file must be uploaded to Oracle ILOM prior to enabling the Strict Certificate Mode property. **CLI Certificate Show Syntax**: **show /***SP*|*CMM***/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 TABLE: File Transfer Methods on page 37.
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*|*CMM***/clients/activedirectory/cert clear_action= true** -or- **reset /***SP*|*CMM***/clients/activedirectory/cert** When prompted, type y to delete or n to cancel the action.

TABLE: Optionally Configuring Active Directory Groups

User Interface Configurable Target:

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

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

User Interface Configurable Target:

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

Property	Description
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*|*CMM***/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''

TABLE: Optionally Configuring Active Directory Groups *(Continued)*

User Interface Configurable Target:

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

Property	Description
Custom Groups (/customgroups/*1*|*2*|*3*|*4*|*5*)	A system administrator can optionally configure up to five Custom Group properties in Oracle ILOM to provide user authorization. Oracle ILOM uses the Custom Group properties to determine the appropriate user roles to assign when authenticating users who are members of a Custom Group. When enabling the use of Custom Groups in Oracle ILOM, both the Roles property and the Custom Groups property must be configured. For further information about the configuration properties for Roles, see the Roles property in TABLE: Enabling Active Directory Authentication on page 41. **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*|*CMM***/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" on page 30
Save	**Web interface** – To apply changes made to properties in the Admin, Operator, or Custom Group dialogs, you must click Save.

TABLE: Configuring Active Directory User Domains

User Interface Configurable Target:

- **CLI**: /*SP*|*CMM*/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 **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. **CLI User Domains Syntax:** **set /***SP*|*CMM***/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: Optionally Configuring Active Directory Alternate Servers

User Interface Configurable Target:

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

Property	Description
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 TABLE: Enabling Active Directory Authentication on page 41. **CLI Alternate Server Address and Port syntax:** **set /***SP*|*CMM***/clients/activedirectory/alternateservers/***n* **address=** *sting* **port=***string* **CLI Alternate Server Certificate Syntax:** **show /***SP*|*CMM***/clients/activedirectory/alternateservers/***n***/cert** **load_uri=***file_transfer_method***://***host_address***/***file_path***/***filename* **set /***SP*|*CMM***/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: Optionally Editing DNS Locator Queries

User Interface Configurable Target:

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

Property	Default Value	Description
DNS Locator Queries (/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*|*CMM*/clients/activedirectory/dnslocatorqueries/1** **set /*SP*|*CMM*/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: Guidelines for Troubleshooting Active Directory Authentication

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

- To test and diagnose Active Directory authentication, follow these steps:

  1: Set the Active Directory Log Details property to `trace`.

  2: Attempt an authentication to Oracle ILOM to generate events.

  3: Review the Oracle ILOM event log file.
- Ensure that the user groups and user domains configured on the Active Directory server match the user groups and user domains configured in Oracle ILOM.
- The Oracle ILOM Active Directory Client does not manage clock settings. The clock settings in Oracle ILOM are configurable manually or through an NTP server.

  Note. When the clock settings in Oracle ILOM are configured using an NTP server, Oracle ILOM performs an ntpdate using the NTP server(s) before starting the NTP daemon.

Related Information:

- TABLE: Enabling Active Directory Authentication on page 41
- *Oracle ILOM 3.1 User's Guide*, "Managing Oracle ILOM Log Entries" on page 45
- "Setting Properties for SP or CMM Clock" on page 108

Configuring LDAP/SSL

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

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

TABLE: Enabling LDAP/SSL Authentication

User Interface Configurable Target:

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

Property	Default Value	Description
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*|*CMM***/clients/ldapssl/ state=***disabled*|*enabled*
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. **CLI Roles Syntax**: **set /***SP*|*CMM***/clients/ldapssl/ defaultrole=** *administrator*|*operator*|*a*|*u*|*c*|*r*|*o*|*s*|*none* **Related Information:** • TABLE: Privileges Granted by a User Profile on page 31 • TABLE: Privileges Granted by Individual User Roles on page 32 • TABLE: Optionally Configuring LDAP/SSL Groups on page 58

TABLE: Enabling LDAP/SSL Authentication *(Continued)*

User Interface Configurable Target:

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

Property	Default Value	Description
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*|*CMM***/clients/ldapssl/ address=***LDAP/SSL_server ip_address*|*active_directory_server_dns_host_name* **Related Information:** • TABLE: DNS Configuration Properties on page 101
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*|*CMM***/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*|*CMM***/clients/ldapssl/ timeout=***number_of_seconds*

TABLE: Enabling LDAP/SSL Authentication *(Continued)*

User Interface Configurable Target:

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

Property	Default Value	Description
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*|*CMM***/clients/ldapssl/ strictcertmode=***disabled*|*enabled* **Related Information**: • TABLE: Uploading or Removing an LDAP/SSL Certificate File on page 56
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*|*CMM***/clients/ldapssl/optionalUsermapping/ attributeInfo=<string> searchbase=<string> binddn=cn=***proxyuser***, ou=***organization _name,* **dc=***company***, dc=com bindpw=***password*

TABLE: Enabling LDAP/SSL Authentication *(Continued)*

User Interface Configurable Target:

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

Property	Default Value	Description
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*|*CMM***/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: Uploading or Removing an LDAP/SSL Certificate File

User Interface Configurable Target:

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

Property	Default Value	Description
Certificate File Status (certstatus=)	Read-only	*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*|*CMM***/clients/ldapssl/cert**

TABLE: Uploading or Removing an LDAP/SSL Certificate File *(Continued)*

User Interface Configurable Target:

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

Property	Default Value	Description
File Transfer Method	Browser (web interface only)	*Browser* | *TFTP* | *FTP* | *SCP* | *Paste* For a detailed description of each file transfer method, see TABLE: File Transfer Methods on page 37.
Load Certificate (load_uri=)		**Web interface** – Click the Load Certificate button to upload the LDAP/SSL certificate file that is designated in the File Transfer Method property. **CLI Load Certificate Syntax**: **load_uri=***file_transfer_method***://***host_address***/***file_path***/***filename*
Remove Certificate (clear_action=true)		**Web interface –** Click the Remove Certificate button to remove the LDAP/SSL certificate file presently stored in Oracle ILOM. When prompted, click Yes to continue the action or No to cancel the action. **CLI Remove Certificate Syntax**: **set /***SP*|*CMM***/clients/ldapssl/cert clear_action=true** -or- **reset /***SP*|*CMM***/clients/ldapssl/cert** When prompted, type y to continue the action or n to cancel the action.

TABLE: Optionally Configuring LDAP/SSL Groups

User Interface Configurable Target:

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

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

User Interface Configurable Target:

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

Property	Description
Custom Groups (/customgroups/*1*|*2*|*3*|*4*|*5*)	A system administrator can optionally configure up to five Custom Groups properties in Oracle ILOM to provide user authorization. Oracle ILOM uses the Custom Group properties to determine the appropriate user roles to assign when authenticating users who are members of a Custom Group When enabling the use of Custom Groups in Oracle ILOM, both the Roles property and the Custom Groups property must be configured. For further information about the configuration properties for Roles, see the Roles property in TABLE: Enabling LDAP/SSL Authentication on page 53. **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|CMM***/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" on page 30
Save	**Web interface** – To apply changes made to properties in the Admin, Operator, or Custom Group dialogs, you must click Save.

TABLE: Configuring LDAP/SSL User Domains

User Interface Configurable Target:

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

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

User Interface Configurable Target:

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

Property	Description
Alternate Servers (/*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*|*CMM***/clients/ldapssl/alternateservers/***n* **address=***sting* **port=** *string* **CLI Alternate Server s Certificate Syntax:** **show /***SP*|*CMM***/clients/ldapssl/alternateservers/***n***/cert load_uri=***file_transfer_method***://***host_address***/***file_path***/***filename* **set /***SP*|*CMM***/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: Guidelines for Troubleshooting LDAP/SSL Authentication

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

- To test LDAP/SSL authentication and set the Oracle ILOM event log to trace LDAP/SSL events, follow these steps:

  1: Set the LDAP/SSL Log Details property to trace.

  2: Attempt an authentication to Oracle ILOM to generate events.

  3: Review the Oracle ILOM event log file.
- Ensure that the user groups and user domains configured on the LDAP/SSL server match the user groups and user domains configured in Oracle ILOM.
- The Oracle ILOM LDAP/SSL Client does not manage clock settings. The clock settings in Oracle ILOM are configurable manually or through an NTP server.

  Note. When the clock setting in Oracle ILOM is configured using an NTP server, Oracle ILOM performs an ntpdate using the NTP server(s) before starting the NTP daemon.

Related Information:

- TABLE: Enabling LDAP/SSL Authentication on page 53
- *Oracle ILOM 3.1 User's Guide*, "Managing Oracle ILOM Log Entries" on page 45
- "Setting Properties for SP or CMM Clock" on page 108

Configuring LDAP

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

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

- TABLE: Requirements for Enabling Oracle ILOM as an LDAP Client on page 63
- TABLE: Enabling Oracle ILOM to Use LDAP Authentication on page 64

TABLE: 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: Enabling Oracle ILOM to Use LDAP Authentication

User Interface Configurable Target:

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

Property	Default Value	Description
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*|*CMM***/clients/ldap/ state=***disabled*|*enabled*
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*|*CMM***/clients/ldap/ defaultrole=** *administrator*|*operator*|*a*|*u*|*c*|*r*|*o*|*s* **Related Information:** • TABLE: Privileges Granted by a User Profile on page 31 • TABLE: Privileges Granted by Individual User Roles on page 32
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*|*CMM***/clients/ldap/ address=***ldap_server ip_address*|*ldap_server_dns_host_name* **Related Information:** • TABLE: DNS Configuration Properties on page 101

TABLE: Enabling Oracle ILOM to Use LDAP Authentication *(Continued)*

User Interface Configurable Target:

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

Property	Default Value	Description
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*|*CMM***/clients/ldap/ port=***number*
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*|*CMM***/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*|*CMM***/clients/ldap/ binddn=cn=***proxyuser*, **ou=***organization_name*, **dc=***domain*
Bind Password (bindpw=)		To provide Oracle ILOM with a password for the read-only proxy user, populate the Bind Password property with a password. **CLI Bind Password Syntax**: **set /***SP*|*CMM***/clients/ldap/ bindpw=***password*
Save		**Web interface** – To apply changes made to properties within the LDAP Settings page, you must click Save.

Configuring RADIUS

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

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

TABLE: Enabling Oracle ILOM to Use RADIUS Client Server Authentication

User Interface Configurable Target:

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

Property	Default Value	Description
State (state=)	Disabled	*Disabled* | *Enabled* To configure Oracle ILOM as a RADIUS client. set the State Property to Enabled. When the State property is enabled, Oracle ILOM sends user login data to the RADIUS server for user authentication and authorization. **CLI RADIUS State Syntax**: **set /***SP*|*CMM***/clients/radius/ state=***disabled*|*enabled*
Roles (defaultrole=)	Operator	*Administrator* | *Operator* | *Advanced* To define which features in Oracle ILOM are accessible to RADIUS authenticated users, set the default Roles property to one of the three Oracle ILOM user roles: Administrator (a | u | c | r | o), Operator (c | r | o), Advanced (*a* | *u* | *c* | *r* | *o* | *s*). Authorization levels for using features within Oracle ILOM are dictated by the privileges granted by the configured Oracle ILOM user role. For a description of privileges assigned, see the user role and user profile tables listed in the Related Information section below. **CLI Roles Syntax**: **set /***SP*|*CMM***/clients/radius/ defaultrole=** *administrator*|*operator*|*a*|*u*|*c*|*r*|*o*|*s* **Related Information:** • TABLE: Privileges Granted by a User Profile on page 31 • TABLE: Privileges Granted by Individual User Roles on page 32

TABLE: Enabling Oracle ILOM to Use RADIUS Client Server Authentication *(Continued)*

User Interface Configurable Target:

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

Property	Default Value	Description
Address (address=)	0.0.0.0	*IP address*	*DNS host name* (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. **CLI Address Syntax**: **set /***SP*|*CMM***/clients/radius/ address=***radius_server ip_address*|*ldap_server_dns_host_name* **Related Information:** • TABLE: DNS Configuration Properties on page 101
Port (port=)	1812	*1812*	*User-specified TCP port* TCP port 1812 is used by Oracle ILOM to communicate with the RADIUS server. If necessary, configure Oracle ILOM to use another port by modifying the default Port number: 1812 **CLI Port Syntax**: **set /***SP*|*CMM***/clients/radius/ port=***number*
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*|*CMM***/clients/radius/ secret=***password*
Save		**Web interface**. To apply changes made to properties within the RADIUS Settings page, you must click Save.

Modifying Default Settings for Network Deployment and Administration

Description	Links
Refer to this section to better understand Oracle ILOM's deployment options and default settings for management access and network connectivity.	• "Network Deployment Principles and Considerations" on page 70
Refer to this section for management access requirements and configuration properties.	• "Modifying Default Management Access Configuration Properties" on page 78
Refer to this section for connectivity requirements and configuration properties.	• "Modifying Default Connectivity Configuration Properties" on page 92
Refer to these sections for instructions on how to set up system identification labels and set the date and time properties in Oracle ILOM.	• "Assigning System Identification Information" on page 107 • "Setting Properties for SP or CMM Clock" on page 108
Refer to this section for guidelines for resolving management access and network connectivity issues.	• "Suggested Resolutions for Network Connectivity Issues" on page 110

Related Information

- *Oracle ILOM 3.1 Security Guide*, deployment considerations
- *Oracle ILOM 3.1 User's Guide*, "Logging In to Oracle ILOM" on page 10

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:

Management Access 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: Management Access Deployment Options and Default Settings

Management Access	Management Service	Defaults	Description
Web browser client	• Web Server	• HTTPS over port 443 enabled • TLSv1, enabled • SSL certificate & self-signing keys • Client timeout session, 15 minutes	The Web Server management service in Oracle ILOM, by default, enables a secure communication channel between a web browser client and the Oracle ILOM SP or CMM. Network administrators can accept the default web server properties provided in Oracle ILOM or choose to modify them as needed. **Related Information:** • "Use of Web Server Certificates and SSH Server-Side Keys" on page 75 • TABLE: Web Server Configuration Properties on page 79 • "Resolving Web Browser Security Settings" on page 110
Command-line SSH client	• Secure Shell (SSH) Server	• Port 22 enabled • Generated SSH keys • Client timeout session, unlimited	The SSH Server service in Oracle ILOM uses server-side keys to encrypt the management channel between an SSH command-line client and an Oracle ILOM SP or CMM. Oracle ILOM automatically generates the server-side SSH keys on the first boot of a factory default system. **Related Information:** • TABLE: SSH Server Configuration Properties on page 88 • "Use of Web Server Certificates and SSH Server-Side Keys" on page 75

TABLE: Management Access Deployment Options and Default Settings *(Continued)*

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	The SNMP management service in Oracle ILOM offers a secure protocol management solution for monitoring and managing Oracle servers. All SNMP monitoring and management functionality is accessible from an SNMP application, such as Net-SNMP. Prior to using the SNMP management service in Oracle ILOM, one or more Oracle ILOM user accounts must be created. Additionally, prior to using SNMP sets, the SNMP sets property must be enabled. Oracle ILOM is shipped with SNMPv3 enabled, although administrators can optionally choose to enable the properties for SNMPv1 or SNMPv2c. **Related Information:** • TABLE: SNMP Configuration Properties on page 84 • *Oracle ILOM 3.1 Protocol Management Reference Guide*, "Configuring SNMP Settings in Oracle ILOM" on page 9 • "Alert Notification Configuration Properties" on page 164 • Net-SNMP (`http://net-snmp.sourceforge.net/`)

TABLE: Management Access Deployment Options and Default Settings *(Continued)*

Management Access	Management Service	Defaults	Description
IPMItool client	• IPMI	• IPMPv2 over port 623, enabled • Service state enabled	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:** • TABLE: IPMI Service Configuration Properties on page 89 • "Assignable Oracle ILOM User Roles" on page 30 • Oracle ILOM 3.1 Protocol Management Reference, Server Management Using IPMI • "Alert Notification Configuration Properties" on page 164 • IPMItool (`http://ipmitool.sourceforge.net/`)
Web service management client	• WS-Management (WS-Man)	• HTTP* over Port 8899 enabled • Service state enabled	The WS-Management service in Oracle ILOM offers a standard web-service interface for: • Monitoring the health of Oracle servers • Reporting inventory status • Remotely managing the power on a host server • Remotely resetting the Oracle ILOM SP The WS-Man configurable options in Oracle ILOM include the transfer protocol mode (HTTP or HTTPS), the communication port (8899 or 8888), and the service state. Network administrators can accept the default WS-Man properties provided in Oracle ILOM or modify them as needed. **Related Information:** • "Use of Web Server Certificates and SSH Server-Side Keys" on page 75 • TABLE: WS-Man Web Service Configuration Properties on page 91 • *Oracle ILOM 3.1 Protocol Management Reference Guide*, "Server Management Using WS-Management and CIM" on page 133

* To maximize security, HTTPS over port 8888 is the preferred transfer protocol mode.

Connectivity Deployment Options

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

TABLE: Connectivity Deployment Options and Default Settings

Connectivity Options	Defaults	Description
Network	• IPv 4, DHCP enabled • IP 6, Stateless enabled • Management Port: MGMT	Oracle ILOM, by default, arrives configured to operate in a dual-stack IPv4 and IPv6 network environment. Upon setting a physical network management connection to the server or CMM, Oracle ILOM will attempt to learn the physical address for the SP or CMM from the IP mapping and routing devices configured on the network. Network administrators can accept the default dual-stack IP network properties in Oracle ILOM, or choose to disable them and configure the required IP network properties. **Related Information:** • TABLE: Network Connectivity Configuration Properties on page 93 • "Sideband Network Management Connection" on page 4 • "Dedicated Network Management Connection (Default)" on page 2
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:** • TABLE: DNS Configuration Properties on page 101 • "Example Setup of Dynamic DNS" on page 103
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. **Related Information:** • TABLE: Serial Port Configuration Properties on page 103 • "Serial Management Port Owner" on page 76 • "Dedicated Network Management Connection (Default)" on page 2

Use of Web Server Certificates and SSH Server-Side Keys

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

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

For further details about web server certificate configuration properties, see TABLE: SSL Certificate and Private Key Configuration Properties for HTTPS Web Server on page 82.

For further details about SSH server-side key configuration properties, see TABLE: SSH Server Configuration Properties on page 88.

Default Timeout for CLI and Web Sessions

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

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

For CLI session timeout configuration properties, see TABLE: CLI Session Timeout Configuration Property on page 90. For web session timeout configuration properties, see TABLE: Web Server Configuration Properties on page 79.

Displaying Banner Messages at Log-In

The Banner Message properties in Oracle ILOM enable network administrators to display important messages to Oracle ILOM users when they log in. For instance, network administrators can use this message display functionality to alert users of special access restrictions, provide notices of upcoming system maintenance, and for other similar purposes.

The Oracle ILOM web and CLI banner messages can appear at pre-login or immediately after login. To configure a banner message and enable its display, see TABLE: Banner Message Configuration Properties on page 92.

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 TABLE: Serial Port Configuration Properties on page 103.

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: Oracle ILOM Default Network Ports

Port	Protocol	Application
Common Network Ports		
22	SSH over TCP	SSH - Secure Shell
25	SMTP over TCP	SMTP client communication
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol (outgoing)
80	HTTP over TCP	Web (user-configurable)
123	NTP over UDP	NTP - Network Time Protocol (outgoing)
161	SNMP over UDP	SNMP - Simple Network Management Protocol (user-configurable)
162	IPMI over UDP	IPMI - Platform Event Trap (PET) (outgoing)
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)
8888	WS-Man over HTTPS	WS-Man Service
8889	WS-Man over HTTP	WS-Man Service
SP Network Ports		
5120	TCP	Oracle ILOM Remote Console: CD
5121	TCP	Oracle ILOM Remote Console: Keyboard and Mouse
5123	TCP	Oracle ILOM Remote Console: Diskette
5555	TCP	Oracle ILOM Remote Console: Encryption
5556	TCP	Oracle ILOM Remote Console: Authentication
6481	TCP	Oracle ILOM Remote Console: Servicetag Daemon
7578	TCP	Oracle ILOM Remote Console: Video
7579	TCP	Oracle ILOM Remote Console: Serial
CMM Network Ports		
8000 - 8023	HTTP over TCP	Oracle ILOM drill-down to server modules (blades)

TABLE: Oracle ILOM Default Network Ports *(Continued)*

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

Legacy Oracle Servers Not Supporting IPv6

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

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

Modifying Default Management Access Configuration Properties

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

TABLE: Web Server Configuration Properties

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
HTTP Webserver (`http/ securedirect= enabled servicestate= disabled`)	Redirect Connection to HTTPS	*Redirect Connection to HTTPS* | *Enabled* | *Disabled* When the HTTP Webserver property is set to Redirect Connection to HTTPS, the service state property for HTTPS Webserver is automatically enabled. These default property values instruct Oracle ILOM to use HTTPS to securely transmit information to the web server. When the HTTP Webserver property is set to enabled, Oracle ILOM uses HTTP a non-encrypted protocol to transmit information to the web server. When the HTTP Webserver property is set to disabled, the use of the transmitting information to the web server using HTTP is disabled in Oracle ILOM. **CLI Syntax for HTTP Web Server**: **set /***SP|CMM***/services/http securedirect=***enabled|disabled*** servicestate=***disabled|enabled
HTTP Port (`http/ port=`)	80	*80* | *User_defined* When the HTTP service state is enabled, Oracle ILOM by default, communicates with the web server using HTTP over TCP port 80. If necessary, the default port number can be changed. **CLI Syntax for HTTP Port**: **set /***SP|CMM***/services/http port=<***n***>**

TABLE: Web Server Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
HTTP Session Timeout (`http/ sessiontimeout =`)	15 seconds	*15 seconds* | *User_defined* The HTTP web session timeout determines how many minutes until an inactive web browser client is automatically logged out. The default HTTP web session timeout is 15 minutes. If necessary, the default session timeout value can be increased or decreased. **CLI Syntax for HTTP Session Timeout**: **`set /`***SP|CMM*`/services/http sessiontimeout=<`***n***`>`**
HTTPS Webserver (`https/ servicestate= enabled`)	Enabled	*Enabled* | *Disabled* When the HTTPS Webserver property is set to enabled, Oracle ILOM uses HTTPS to securely transmit information to the web server. When the HTTPS Webserver property is set to disabled, the use of transmitting information to the web server using HTTPS is disabled in Oracle ILOM. **CLI Syntax for HTTPS Web Server**: **`set /`***SP|CMM*`/services/https servicestate=`***enabled|disabled***
HTTPS Port (`https/ port=`)	443	*443* | *User_defined* When the HTTPS service state is enabled, Oracle ILOM, by default, communicates with the web server using HTTPS over TCP port 443. If necessary, the default port number can be changed. **HTTPS Port CLI Syntax**: **`set /`***SP|CMM*`/services/https port=<n>`**
HTTPS Session Timeout (`https/session timeout=`)	15 seconds	*15 seconds* | *User_defined* The HTTPS web session timeout determines how many minutes until an inactive web browser client is automatically logged out. The default HTTPS web session timeout is 15 minutes. If necessary, the default session timeout value can be increased or decreased. **CLI Syntax for HTTPS Session Timeout**: **`set /`***SP|CMM*`/services/https sessiontimeout=<`***n***`>`**
SSLv2 (`https/ sslv2= disabled`)	Disabled	*Disabled* | *Enabled* The SSLv2 property is disabled by default. If necessary, the default SSLv2 property can be enabled. **CLI Syntax for SSLv2:** **`set /`***SP|CMM*`/services/https sslv2=`***disabled|enabled***

TABLE: Web Server Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
SSLv3 (https/ sslv3= enabled)	Enabled	*Enabled	Disabled* Oracle ILOM by default uses SSLv3 and TLSv1 to enable the strongest secure socket layer encryption. If necessary, the default SSLv3 property can be disabled. **CLI Syntax for SSLv3:** **set /***SP	CMM***/services/https sslv3=***enabled	disabled*
TLSv1 (https/ tlsv1= enabled)	Enabled	*Enabled	Disabled* Oracle ILOM by default uses SSLv3 and TLSv1 to enable the strongest secure socket layer encryption. If necessary, the default TLSv1 property can be disabled. **CLI Syntax for TLSv1:** **set /***SP	CMM***/services/https tlsv1=***enabled	disabled*
Weak Ciphers (https/ weak_ciphers= disabled)	Disabled	*Disabled	Enabled* The Weak Ciphers property is disabled by default. It might be necessary to enable weak ciphers to support the use of older web browsers. **CLI Syntax for Weak Ciphers:** **set /***SP	CMM***/services/https weak_ciphers=***disabled	enabled* **Related Information:** • "Resolving Web Browser Security Settings" on page 110
Save		**Web interface** – To apply changes made to properties within the Web Server Settings page, you must click Save.

TABLE: SSL Certificate and Private Key Configuration Properties for HTTPS Web Server

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

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

Property	Default Value	Description
Certificate File Status (certstatus=)	Using Default (No custom certificate or private key loaded)	*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: • Default SSL certificate and private self-signed 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. The default self-signed SSL certificate ensures that all communication between a web browser client and the Oracle ILOM SP (or CMM) is fully encrypted. **CLI Syntax to Show Certificate Status**: **show** /*SP*|*CMM***/https/ssl**
Custom Certificate Load (/custom_certificate)		**Web interface** – Click the Load Certificate button to upload the Custom Certificate file that is designated in the File Transfer Method properties. **Note.** A valid custom certificate configuration requires the uploading of a custom certificate and a custom private key. Only then will the custom SSL certificate configuration apply and be persistent across system reboots and Backup and Restore operations. **CLI Syntax to Load Custom Certificate**: **load_uri=** *file_transfer_method***://***host_address***/***file_path***/***custom_certificate_filename* Where f*ile_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" on page 36.

TABLE: SSL Certificate and Private Key Configuration Properties for HTTPS Web Server *(Continued)*

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

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

Property	Default Value	Description
Custom Certificate Remove (/custom_certificate clear_action=true)		**Web interface –** Click the Remove Certificate Button to remove the Custom SSL Certificate file presently stored in Oracle ILOM. When prompted, click Yes to delete or No to cancel action. **CLI Syntax to Remove Certificate**: **set /*SP*|*CMM*/services/https/ssl/custom_certificate clear_action=true** When prompted, type y to delete or n to cancel action.
Custom Private Key (/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_filename* 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" on page 36.
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*|*CMM*/services/https/ssl/custom_key clear_action=true** When prompted, type y to delete or n to cancel the action.

TABLE: SNMP Configuration Properties

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

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

Property	Default Value	Description
State (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*|*CMM***/services/snmp state=***enabled*|*disabled*
Port (port=)	161	*161*	*User_specified.* Oracle ILOM, by default, uses TCP port 161 to transmit SNMP communication between an Oracle ILOM SP (or Oracle ILOM CMM) and the network. If necessary, the default port property number can be changed. **CLI Syntax for SNMP Port**: **set /***SP*|*CMM***/services/snmp port=***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.

TABLE: SNMP Configuration Properties *(Continued)*

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

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

Property	Default Value	Description
Set Requests (sets=)	Disabled	*Disabled* | *Enabled* The Set Requests property is disabled in Oracle ILOM by default. When the Sets Requests property is disabled, the following SNMP MIBs are available for monitoring purposes: • SUN-HW-TRAP-MIB – Use this MIB to monitor trap notifications for hardware-related events such as faults. • SUN-PLATFORM-MIB – Use this MIB to poll hardware-related information such as inventory and health. When the Set Requests property is enabled, the MIBs described above are available for monitoring purposes and the following MIBs are available for management purposes: • SUN-HW-CTRL-MIB – Use this MIB to configure hardware policies such as power management. • SUN-ILOM-CONTROL-MIB – Use this MIB to configure Oracle ILOM features such as creating users and configuring services. **CLI Syntax for Set Requests**: **set /SP|CMM/services/snmp sets=***disabled* | *enabled* **Related Information**: • Oracle ILOM 3.1 Protocol Management Reference, Server Management Using SNMP
Protocols (v1 | v2c | v3)	v3, Enabled	*v1* | *v2c* | *v3* Oracle ILOM, by default, enables the use of SNMP v3 and disables the use of SNMP v1 and v2c. SNMPv1 and v2c do not support encryption and use community strings as a form of authentication. SNMPv3 uses encryption to provide a secure channel and uses individual user names and passwords that are stored securely on the SNMP management station. If necessary, the default SNMP Protocol property value is configurable. **Note -** Use SNMP v2c or v3 for monitoring purposes and keep the default property disabled for Set Requests. **CLI Syntax to Modify Default Protocol:** **set /SP|CMM/services/snmp** *v1* | *v2c* | *v3***=***enabled* | *disabled*
Save		**Web interface** – To apply changes made to properties within the SNMP Management page, you must click Save.

TABLE: SNMP Configuration Properties *(Continued)*

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

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

Property	Default Value	Description
SNMP Communities (/communities)		*Community Name* | *Permission= Read-only* (ro) | *Read-write* (rw) SNMP communities apply only to SNMP v1 or v2c to control user access and authorization levels in Oracle ILOM. When the Protocols property for SNMP v1 or v2c is enabled, the properties for SNMP communities are configurable in Oracle ILOM. The following rules apply when configuring communities: • Community name – Up to 35 characters in length, must start with an alphabetic character, and must not contain any spaces • Save (web interface only) – All changes made within the SNMP Add SNMP User dialog must be saved **CLI Syntax to Create SNMP Communities**: **create /***SP*|*CMM***/services/snmp/communities name=***community_name* **permission=***rw*|*ro* **show /***SP*|*CMM***/services/snmp/communities** *public*|*private* **delete /***SP*|*CMM***/services/snmp/communities** *community_name*

TABLE: SNMP Configuration Properties *(Continued)*

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

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

Property	Default Value	Description
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 – Up to 35 characters in length, must start with an alphabetic character, and must not contain any spaces • Authentication or privacy password – Up to 16 characters in length, case-sensitive, no colons, no spaces, and password must be confirmed • 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|CMM***/services/snmp/***[new_username] **authenticationprotocol=***[MD5|SHA]* **authenticationpassword=***[changeme]* **permission=***[ro|rw]* **privacyprotocol=***AES|DES|none* privacypassword=*[user_password]* **show /***SP|CMM***/services/snmp/users** **delete /***SP|CMM***/services/snmp/username**
MIBs Download (/mibs dump_uri=)		Oracle ILOM provides the ability to download the SUN SNMP MIBs directly from the server SP or CMM.

TABLE: SSH Server Configuration Properties

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
State (state=)	Enabled	*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 (or Oracle ILOM CMM) using a command-line interface. When the SSH Server State property is disabled or restarted, all CLI SP or CLI CMM sessions running over SSH are automatically terminated. **Note.** Oracle ILOM automatically generates the SSH Server side keys on the first boot of a factory default system. **Web interface:** Changes to the SSH Server State in the web interface do not take affect in Oracle ILOM until you click Save. **CLI Syntax for SSH Server State**: **set /***SP*|*CMM***/services/ssh state=** *enabled*|*disabled*
Restart Button (restart_sshd_action=)		*True*|*False* Restarting the SSH server will automatically: (1) terminate all connected SP or CMM CLI sessions, as well as (2) activate newly pending server-side key(s). **CLI Syntax for Restart:** **set /***SP*|*CMM***/services/ssh restart_sshd_action=true**
Generate RSA Key Button (generate_new_key_type=rsa generate_new_key_action= true)		Provides the ability to generate a new RSA SSH key. **CLI Syntax for Generate RSA Key**: **set /***SP*|*CMM***/services/ssh generate_new_key_type=rsa generate_new_key_action=true**
Generate DSA Key Button (generate_new_key_type=dsa generate_new_key_action=)		Provides the ability to generate a new DSA SSH key. **CLI Syntax for Generate DSA Key:** **set /***SP*|*CMM***/services/ssh generate_new_key_type=dsa generate_new_key_action=true**

TABLE: IPMI Service Configuration Properties

User Interface Configurable Target:

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

User Roles:

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

Property	Default Value	Description
State (state=)	Enabled	*Enabled* | *Disabled* The State property for IPMI v2 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 (or Oracle ILOM CMM) using a command-line interface. When the IPMI State property is disabled, all IPMItool clients connected to the SP or CMM through the Oracle ILOM CLI are automatically terminated. **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*|*CMM***/services/ipmi state=** *enabled*|*disabled*

TABLE: CLI Session Timeout Configuration Property

User Interface Configurable Target:

- **CLI**: /*SP*|*CMM*/cli
- **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
Session Timeout (timeout=)	Disabled	*Disabled* | *Enabled, minutes=n* The CLI Session Timeout property determines how many minutes until an inactive CLI session is automatically logged out. By default, there is no CLI timeout configured. If the Oracle ILOM CLI is used on a shared console, network administrators are recommended to set the CLI session timeout value to 15 minutes or less. **Web interface:** Changes to the CLI session timeout properties in the web interface do not take affect in Oracle ILOM until you click Save. **CLI Syntax for CLI Session Timeout**: **set /***SP*|*CMM***/cli timeout=***enabled*|*disabled* **minutes=***value*

TABLE: WS-Man Web Service Configuration Properties

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
State (state=)	Enabled	*Enabled*	*Disabled* The WS-Man web service State property is enabled by default. If necessary, the WS-Man web service state can be disabled. **Web interface:** Changes to the WS-Man state in the web interface do not take affect in Oracle ILOM until you click Save. **CLI Syntax for WS-Man State**: **set /***SP*|*CMM***/services/wsman state=***enabled*|*disabled* **Related Information:** • "Server Management Using WS-Management and CIM" on page 133
Mode (mode=http)	HTTP	*HTTP*|*HTTPS* The Mode property is set to HTTP by default. To improve security, this default property value can be set to HTTPS. **CLI Syntax for WS-Man Mode:** s**et /***SP*|*CMM***/services/wsman mode=***http*|*https*
HTTP Port (http_port=)	8889	*8889*	*user_defined* When the State property is enabled and the Mode property is set to HTTP, Oracle ILOM uses TCP port 8889 for the WS-Man web service. If necessary, the default port property value can be changed. **CLI Syntax for WS-MAN HTTP Port**: **set /***SP*|*CMM***/services/wsman http_port=***n*
HTTPS Port (https_port=)	8888	*8888*	*user_defined* When the State property is enabled and the Mode property is set to HTTPS, Oracle ILOM uses TCP port 8888 for the WS-Man web service. If necessary, the default port property value can be changed. **CLI Syntax for WS-Man HTTPS Port**: **set /SP|CMM/services/wsman https_port=***n*

TABLE: Banner Message Configuration Properties

User Interface Configurable Target and User Role:

- **CLI**: `/SP|CMM/preferences/banner`
- **Web**: ILOM Administration > Management Access > Banner Messages
- **User Role:** admin (a) (required for property modification)

Property	Default Value	Description
Connect Message (`connect_message=`)		Populate the Connect Message property with content to appear in the Oracle ILOM interfaces upon connecting to Oracle ILOM. **CLI Syntax to Set Connect Message:** **`set /SP/preferences/banner connect_message=`***<content>*
Login Message (`login_message=`)		Populate the Login Message property with content to appear in the Oracle ILOM interfaces after logging into Oracle ILOM. **CLI Syntax to Set Login Message:** **`set /SP/preferences/banner login_message=`***<content>*
Login Message Acceptance (`login_message_acceptance=`)	Disabled	*Disabled* | *Enable*d Set the Login Banner Acceptance property to enabled to display the banner message. **CLI Syntax for Login Message Acceptance:** **`set /SP/preferences/banner login_message_acceptance=`** *disabled* | *enabled*

Modifying Default Connectivity Configuration Properties

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

- TABLE: Network Connectivity Configuration Properties on page 93
- TABLE: DNS Configuration Properties on page 101
- TABLE: Serial Port Configuration Properties on page 103

TABLE: Network Connectivity Configuration Properties

User Interface Configurable Target and User Role:

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

Requirements:

- Pending network modifications in the CLI must be committed to take affect in Oracle ILOM.
- Network modifications made in the web 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*|*CMM***/network pendingstate=***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 and CMM are set at the factory. The MAC Address properties for both the SP and CMM are non-configurable read-only properties in Oracle ILOM. **CLI Syntax to Show MAC Address Properties:** **show /***SP*|*CMM***/network**
Management Port (managementport=)	MGMT	*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* **Related Information**: • "Sideband Network Management Connection" on page 4 • "Dedicated Network Management Connection (Default)" on page 2

TABLE: Network Connectivity Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Requirements:

- Pending network modifications in the CLI must be committed to take affect in Oracle ILOM.
- Network modifications made in the web 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 or CMM. Optionally, network administrators can disable the DHCP property and choose to configure a static IPv4 network address, Netmask address and Gateway address for the server SP or CMM. **Note.** When DHCP is set, Oracle ILOM uses the default Auto DNS property to assign the DNS named server and search path. For dual-stack DHCP configurations, the DNS settings in Oracle ILOM can be set to receive DNS information from either the IPv4 or the IPv6 DHCP server. **CLI Syntax for IPv4 IP Discovery Mode**: **set /***SP*|*CMM***/network pendingipdiscoverymode=** *dhcp*|*static* **Related Information**: • TABLE: DNS Configuration Properties on page 101
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. **CLI Syntax for IPv4 DHCP Client ID**: **set /***SP*|*CMM***/network pendingdhcp_clientid=** *none*|*sysid* **Related Information**: • "Assigning System Identification Information" on page 107

TABLE: Network Connectivity Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Requirements:

- Pending network modifications in the CLI must be committed to take affect in Oracle ILOM.
- Network modifications made in the web 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= 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*|*CMM***/network pendingipaddress=***value* **pendingipnetmask=***value* **pendingipgateway=***value* **Related Information**: • "Input Format for IPv4 and IPv6 Addresses" on page 76
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 dual-stack IP translation. **Note** – The IPv6 state must be enabled in Oracle ILOM for dual-stack IP translations. I**CLI Syntax for IPv6 State**: **set /***SP*|*CMM***/network/ipv6 state=***enabled*|*disabled*

TABLE: Network Connectivity Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Requirements:

- Pending network modifications in the CLI must be committed to take affect in Oracle ILOM.
- Network modifications made in the web Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
IPv6 Autoconfig (/ipv6 autoconfig=)	Stateless, Enabled	*Stateless* | *None* The IPv6 Autoconfig property is set to Stateless in Oracle ILOM by default. When the Autoconfig Stateless property is enabled, Oracle ILOM learns the IPv6 address for the server SP or CMM from a network router configured for IPv6. When the IPv6 Autoconfig Stateless property is set to None, Oracle ILOM is prevented from using Autoconfig Stateless to learn the server SP or CMM IPv6 network address. **Special Considerations:** • The IPv6 Autoconfig Stateless options determine the IP address without any IP support from a DHCPv6 server. • The read-only property value for dhcpv6_server_duid= is set to none when only the IPv6 Autoconfig Stateless property is enabled in Oracle ILOM. • The IPv6 Auto config Stateless property can be enabled in Oracle ILOM at the same time when either: DHCPv6_Stateless or DHCPv6_Stateful is enabled. **CLI Syntax for IPv6 Auto Config:** **set /***SP*|*CMM***/network/ipv6 autoconfig=***stateless*|*none*

TABLE: Network Connectivity Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Requirements:

- Pending network modifications in the CLI must be committed to take affect in Oracle ILOM.
- Network modifications made in the web Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
DHCPv6 Autoconfig (/ipv6 autoconfig=)	None, Disabled	*DHCPv6_Stateless* | *DHCP_Stateful* | *None* The DHCPv6 Autoconfig property is disabled (set to None) in Oracle ILOM by default. When this property is set to None, Oracle ILOM is prevented from learning the SP or CMM network address and DNS information from a DHCPv6 server on the network. Optionally, network administrators can choose to have a network connected DHCPv6 server allocate the IPv6 address and DNS information for the SP or CMM by setting the DHCPv6 Autoconfig property in Oracle ILOM to one of the following values: • DHCPv6 Stateless – When enabled, Oracle ILOM uses the DHCPv6 Stateless Autoconfig to learn the IPv6 address and DNS information for the server SP or CMM. • DHCPv6 Stateful – When enabled, Oracle ILOM uses the DHCPv6 stateful Autoconfig to learn the IPv6 address and DNS information for the server SP or CMM. **Special Considerations:** • The IPv6 Autoconfig Stateless property can be enabled in Oracle ILOM at the same time when DHCPv6 Autoconfig is enabled to use either: DHCPv6_Stateless or DHCPv6_Stateful. • 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|CMM*/network/ipv6 autoconfig= *dhcpv6_stateless|dhcpv6_stateful|none*

TABLE: Network Connectivity Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Requirements:

- Pending network modifications in the CLI must be committed to take affect in Oracle ILOM.
- Network modifications made in the web Network Settings page must be saved to take affect in Oracle ILOM.

Property	Default Value	Description
Link-Local IPv6 Address (/ipv6 link_local_ipaddress=)	Read-only	The read-only property for Link-Local IPv6 Address is a non-routable address that you can use to connect to the Oracle ILOM SP (or the CMM) from another IPv6-enabled node on the same network. Oracle ILOM applies the following principles to build the Link-Local Address for the SP or CMM: • Oracle ILOM uses the SP or CMM MAC address in conjunction with the link-local identifier prefix. • Oracle ILOM, at initialization, uses the Duplicate Address Detection (DAD) protocol to ensure that the reported Local-Link address for the SP (or CMM) is unique. **CLI Syntax for Link-Local Address:** **show /***SP*|*CMM***/network/ipv6**
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 or CMM. 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*|*CMM***/network/ipv6 static_ipaddress=** *ipaddress***/***subnetmask*
IPv6 Gateway (/ipv6 ipgateway=)	Read-only	The read-only IPv6 gateway address presented in this property is learned from an IPv6 router on the network. **CLI Syntax for IPv6 Gateway**: **show/** *SP*|*CMM***/network/ipv6**

TABLE: Network Connectivity Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Requirements:

- Pending network modifications in the CLI must be committed to take affect in Oracle ILOM.
- Network modifications made in the web 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 or the CMM. **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|CMM***/network/ipv6**

TABLE: Network Connectivity Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Requirements:

- Pending network modifications in the CLI must be committed to take affect in Oracle ILOM.
- Network modifications made in the web 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 or CMM. To log back in to Oracle ILOM, open a new browser session and enter the newly assigned IPv 4 address. • The IPv6 pending modifications take affect after they are committed or saved. Changes to the autoconfig properties do not need to be committed in the CLI. • Newly learned auto-configuration IPv6 addresses will not affect any Oracle ILOM session currently connected to the managed device (SP or CMM). **CLI Syntax for IPv4 Commit Pending Modification**: **set /***SP|CMM***/network pendingstate=***enabled|disabled* **pendingipdiscovery=***static|dhcp* **pendingipaddress=***value* **pendingipgateway=***value* **pendingipnetmask=***value* **commitpending=true** **CLI Syntax for IPv6 Commit Pending Modifications:** **set /***SP|CMM***/network pendingstate=***enabled|disabled* **pending_static_ipaddress=***ip6_address***/***subnet_mask_length_in_bits* **commitpending=true** **Related Information**: • "Test IPv4 and IPv6 Connectivity" on page 113

TABLE: DNS Configuration Properties

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
Auto DNS via DHCP (`auto_dns=`)	Enabled	*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*|*CMM***`/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*|*CMM***`/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|CMM/clients/dns searchpath=`** *domain_1.com, domain_2.edu, and so on*

TABLE: DNS Configuration Properties *(Continued)*

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
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|CMM/clients/dns timeout=`***n* **Related Topic:** • "Example Setup of Dynamic DNS" on page 103
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|CMM*`/clients/dns retries=`***n*
Save Button (web only)		**Web interface** – Changes made within the DNS Configuration page must be saved in Oracle ILOM before they can take affect.

TABLE: 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" on page 76. **CLI Syntax for Serial Port Owner:** **`set /SP/serial/portsharing owner=`***SP* | *hostserver*
Host Serial Port (`/host pendingspeed= flowcontrol=`)	Baud Rate= 9600 Flow Control= None	`Baud Rate =` *9600* | `Flow Control =` *Software* | *Hardware* | *None* The Host Serial Port properties are configurable on some Oracle servers. The property values for the Host Serial Port option must match the property values set for the serial console port on the host server. Often referred to as serial port 0, COM1, or /dev/ttyS0. **CLI Syntax for Host Serial Port**: **`set /`***SP* | *CMM***`/serial/host pendingspeed=`***value***`flowcontrol=`***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* | *CMM***`/serial/external pendingspeed=`***value*** `commitpending=true`**
Save Button (web only)		**Web interface** – Changes made within the Serial Port Settings page must be saved in Oracle ILOM before they can take affect.

Example Setup of Dynamic DNS

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

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

▼ Example: Set Up DDNS Configuration

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

Assumptions:

The following assumptions apply to this DDNS configuration example:

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

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

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

1. **Install the `bind9` and `dhcp3-server` packages from the Debian distribution.**

   Installing the `dnsutils` package provides access to `dig`, `nslookup`, and other useful tools.

2. **Using `dnssec-keygen`, generate a key to be shared between the DHCP and DNS servers to control access to the DNS data.**

3. **Create a DNS configuration file named** `/etc/bind/named.conf` **that contains the following:**

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

4. **Add empty zone files for the local network.**

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

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

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

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

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

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

References

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

Assigning System Identification Information

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

TABLE: 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=)	None	The Host Name, when defined, helps identify a managed device that is connected to a computer network. The Host Name property value can contain up to 60 characters. It must begin with a letter and contain only alphanumeric, hyphen, and underscore characters. **CLI Syntax for Host Name:** **set /***SP|CMM* **hostname=***value*
System Identifier (/system_identifier=)	None	The System Identifier, when defined, helps identify the managed device in the payload element of an SNMP trap. The System Identifier property value can contain up to 60 characters using any standard keyboard keys except quotation marks. This property is configurable in both the server SP and CMM. **CLI Syntax for System Identifier**: **set /***SP|CMM* **system_identifier=***value*
System Contact (/system_contact=)	None	The System Contact, when defined, helps identify the point-of-contact for the managed device such as the name or email address of the person responsible for the device. The System Contact property value can consist of a text string using any standard keyboard keys except quotation marks. **CLI Syntax for System Contact**: **set /SP|CMM system_contact=***value*

TABLE: Device Identification Configuration Properties *(Continued)*

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
System Location (`/system_location=`)	None	The System Location, when defined, helps identify the physical location of a managed device such as a rack identifier or a data center location. The system location property value can consist of a text string using any standard keyboard keys except quotation marks. **CLI Syntax for System Location**: **`set /`***SP|CMM* **`system_location=`***value*
Physical Presence Check (`/check_physical_presence=`)	Enabled	The Physical Presence Check affects the behavior for recovering the preconfigured Oracle ILOM `root` account password. • Enabled (true) – When enabled, the Locator button on the physical system must be pressed in order to recover the default Oracle ILOM password. • Disabled (false) – When disabled, the default Oracle ILOM administrator password can be reset without pressing the Locator button on the physical system. Refer to the hardware documentation for instructions for proving physical presence. If the hardware documentation does not mention physical presence, contact your Oracle service representative. **CLI Syntax for Physical Presence Check**: **`set /SP|CMM check_physical_presence=`***true|false* **Related Topic:** • TABLE: Recover Preconfigured root Account or root Account Password (CLI only) on page 36
Save Button (web only)		**Web interface** – Changes made within the Identification page must be saved in Oracle ILOM before they can take affect.

Setting Properties for SP or CMM Clock

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: Oracle ILOM Clock Configuration Properties

User Interface Configurable Target and User Role:

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

Property	Default Value	Description
Date and Time (datetime=)	None	Populate the Date property with the month, day, and year. Populate the Time property with the hours and minutes. **CLI Syntax for Date and Time:** **set /***SP|CMM***/clock datetime=***MMDDhhmmYYYY*
Timezones (timezones=)	None	Timezone Abbreviations (PST, EST, and so on) Populate the Timezones property with the appropriate timezone. **CLI Syntax for Timezones**: **set /***SP|CMM***/clock timezones=***3_to_4_characters*
Synchronize Time with NTP Server (usentpserver=)	Disabled	*Enabled|Disabled* Enable this property to instruct Oracle ILOM to synchronize the clock settings with a network NTP service. **Note -** Requires a minimum configuration of one IP address for an NTP server. See NTP server property. **CLI Syntax for Synchronize Time with NTP Server**: **set /***SP|CMM***/clock usentpserver=***enabled|disabled*
NTP Server 1 (2) (/SP/clients/ntp/server*n*=)	None	Populate the Server 1 or the Server 2 properties with the IP address of an NTP server. **CLI Syntax to Set NTP Server IP address**: **set /SP/clients/ntp/server1=***ip_address*
Save Button (web only)		**Web interface** – Changes made within the Clock Settings page and the Timezone Settings page must be saved in Oracle ILOM before they can take affect.

Refer to the Oracle server documentation to determine whether:

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

Suggested Resolutions for Network Connectivity Issues

Resolving Web Browser Security Settings

As of Oracle ILOM 3.1.0, Internet Explorer (IE) 6 users can no longer connect to the web interface without performing one of two tasks:

- **Task 1** – Upgrade browser to IE 7 or later, or another browser that is equivalent or newer.

  - or -

- **Task 2** – Modify the Oracle ILOM web server properties and SSL certificate and key. For instructions, see the following procedure.

▼ Modify Default Web Server Properties to Support Internet Explorer 6

The preconfigured web server self-signed certificate supplied with Oracle ILOM uses a stronger encryption, which is not supported by IE 6.

For users not wanting to upgrade from IE 6 to IE 7, the web server properties in the following procedure must be modified to permit IE 6 connections to the Oracle ILOM web interface.

Before You Begin

- Admin (a) role is required to modify web server properties in Oracle ILOM.

1. **Log in to the Oracle ILOM CLI.**
2. **Enable weak ciphers by typing:**

   `set /`*SP*|*CMM*`/services/https weak_ciphers=enabled`

3. **Upload a custom key by typing:**

   set /*SP*|*CMM***/services/https/ssl/custom_key load_uri=**<*uri_string* >

4. **Upload custom certificate by typing:**

   set /*SP*|*CMM***/services/https/ssl/custom_cert load_uri=**
   <*uri_string*>

Related Information:

- TABLE: Web Server Configuration Properties on page 79

Resolving Connectivity Issues

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

- TABLE: Troubleshooting IPv4 Connectivity Issues on page 111
- TABLE: Troubleshooting IPv6 Connectivity Issues on page 112

TABLE: 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.
Unable to access the Oracle ILOM web interface using the Internet Explorer 6 (IE 6) web browser.	Internet Explorer 6 users must upgrade their browsers or upload a custom certificate and a private key to use SSL in the Oracle ILOM web interface. For instructions on how to upload a custom SSL certificate, refer to the TABLE: SSL Certificate and Private Key Configuration Properties for HTTPS Web Server on page 82.

TABLE: 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`
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.
Unable to access the Oracle ILOM web interface using the Internet Explorer 6 (IE 6) web browser.	Internet Explorer 6 users must upgrade browsers or upload a custom certificate and a private key to use SSL in the Oracle ILOM web interface. For instructions on how to upload a custom SSL certificate, refer to the TABLE: SSL Certificate and Private Key Configuration Properties for HTTPS Web Server on page 82.

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*|*CMM*`/network/test ping=`***`device_ipv4_address_on network`***

    `set /`*SP*|*CMM*`/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:

    a. Click ILOM Administration > Connectivity > Network > Network Tools.

    b. In the tools dialog, select a test type, specify an IP address of a device on the network, then click Test.

Related Information:

- TABLE: Network Connectivity Configuration Properties on page 93

Using Remote KVMS Consoles for Host Server Redirection

Description	Links
Refer to these sections for setting up and using the GUI-based Oracle ILOM Remote Console for host server KVMS redirection.	• "First-Time Setup for Oracle ILOM Remote Console" on page 116 • "Launching and Using the Oracle ILOM Remote Console" on page 122
Refer to these sections for setting up and using the command-line Oracle ILOM Storage Redirection Console for host storage redirection.	• "First Time Setup for Oracle ILOM Storage Redirection CLI" on page 128 • "Launching and Using the Oracle ILOM Storage Redirection CLI" on page 134
Refer to this section for instructions to launch a serial redirection session to the host server operating system.	• "Starting and Stopping a Host Serial Redirection Session" on page 141

Related Information

- *Oracle ILOM 3.1 Security Guide*, Using Remote KVMS Securely

First-Time Setup for Oracle ILOM Remote Console

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

Requirements for Using the Oracle ILOM Remote Console

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

TABLE: Requirements for Using Oracle ILOM Remote Console

Set Up Requirement	Description
KVMS Settings	Configure SP local client properties for keyboard, video, and mouse redirection behavior. **Defaults**: State: enabled, Mouse Mode: absolute, Display Quality: YUV420, Lock Mode: disabled **Related Information**: • "Configure Local Client KVMS Settings" on page 117
Java Runtime Environment	The Java Runtime Environment (1.5 or later) must be installed on the local client system. To download the latest Java Runtime Environment, go to: `http://java.com`.
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 Operating System Web Browsers" on page 24.
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 Console for video redirection. **Related Information**: • "Register 32-Bit JDK Java Plug-In For Windows IE Web Browser" on page 118 • "Register 32-Bit JDK Java Plug-In for Mozilla Firefox Web Browser" on page 119

TABLE: Requirements for Using Oracle ILOM Remote Console *(Continued)*

Set Up Requirement	Description
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 service State property) and to launch the Oracle ILOM Remote 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 Console, users can launch the remote KVMS session using one of the following redirection methods: • **Serial Redirection (SPARC only)** – This option is available for SPARC server SPs only. When enabled, Oracle ILOM presents a text-based console for the serial host server redirections. • **Video Redirection** – This option is available for CMMs, x86 server SPs and SPARC server SPs. This option presents a GUI-based console for the video redirected host server.
Communication TCP/IP Ports Required	The Oracle ILOM Remote 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 SPARC server redirection only. For a complete list of network ports used by Oracle ILOM, see TABLE: Oracle ILOM Default Network Ports on page 77.

▼ Configure Local Client KVMS Settings

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	Description
State (`servicestate=`)	The KVMS service State is enabled by default for redirection. This State property must be enabled to use the Oracle ILOM Remote Console. Disabling this state will also disable the use of the Oracle ILOM Remote Console. **CLI Syntax for KVMS Service State**: **`set /SP/services/kvms servicestate=`***enabled* | *disabled*

Property	Description
Mouse (`mousemode=`)	Set the appropriate mouse mode option: • Relative (default) – Set this local mouse mode setting if your remote host is running the Linux OS. • Absolute – Set this local mouse mode setting if your remote host running the Windows OS or Solaris. **CLI Syntax for KVMS Mouse Mode**: **`set /SP/services/kvms mousemode=`***absolute* | *relative*
Display Quality (`display_quality=`)	Select the appropriate video quality option: • YUV420 (initial factory default) – Select this setting to transmit a higher compressed color image data scheme resulting in an optimized data transfer rate. • YUV444 – Select this setting to transmit a lower compressed color image data scheme resulting in a greater image resolution. • VQ2 – Select this setting to transmit a lower compressed video data scheme that works best for two-color terminal display outputs. • VQ4 – Select this setting to transmit a lower compressed video data scheme that works best for four-color terminal display outputs. **Note -** The set property value for the Display Quality remains persistent after rebooting the SP. Therefore, the initial factory default value (YUV420) is not retained if modifications are made. **CLI Syntax for KVMS Display Quality:** **`set /SP/services/kvms display_quality=`***YUV420* | *YUV444* | *VQ2* | *VQ4*
Host Lock Settings (`lock_mode=`)	For a description of the host lock properties, see "Optionally Set a Lock Mode to Secure the Host Server Desktop" on page 120.

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

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

1. **On the Windows Client, open Windows Explorer (not Internet Explorer).**
2. **In the Windows Explorer dialog box, click Tools > Folder Options, 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. Click the "Always use the selected program to open this kind of file" check box.

d. Click OK, then launch the Oracle ILOM Remote Console.

For instructions, see "Launching and Using the Oracle ILOM Remote Console" on page 122.

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

1. Launch the Oracle ILOM Remote 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 Console button.

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

A dialog for the Java Start Web Program appears.

2. In the Java Start Web Program dialog, do the following:

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

b. Click 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 Console window appears.

For further information on how to redirect KVMS devices using the Oracle ILOM Remote Console, see "Launching and Using the Oracle ILOM Remote Console" on page 122.

Optionally Set a Lock Mode to Secure the Host Server Desktop

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

For a description of lock mode options, as well as how to configure the lock mode in Oracle ILOM, see these topics:

- TABLE: Configurable Host Server Lock Options on page 120
- "Lock Host Desktop When Disconnecting a Remote KVMS Session" on page 121

TABLE: Configurable Host Server Lock Options

Lock Mode Property Values	Description
Windows (`lock_mode=windows`)	The Windows lock option 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) for locking the Windows operating system desktop.
Custom (`lock_mode=custom`)	The Custom lock option 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 CRTL-ALT-DEL 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 lock-key sequence supported by Oracle Solaris or a Linux-based operating system. The custom lock-key sequence needs to be defined on the host operating system prior to enabling the Custom lock mode property in Oracle ILOM. For instructions for creating a custom lock-key sequence, refer to the operating system vendor documentation. • A custom lock-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).
Disabled (`lock_mode=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 the Lock Mode property is set to Custom, proceed to Step 2. Otherwise, if using the web interface proceed to Step 3.

2. **If the Lock Mode property in Step 1 was set to Custom, perform the following to specify a Custom Lock Modifier and a Custom Lock key:**
   - Web – In the KVMS Settings page:

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

     Click the Custom Lock Key list box and select a custom lock key.
   - CLI – Type:

     set /SP/services/kvms lockmodifiers=*value*

     set /SP/services/kvms custom_lock_key=*value*

   Possible Custom Lock Modifier 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 example (Host Lock Configuration) following this procedure.

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

Host Lock Configuration Example:

If the following custom lock key sequence (keyboard shortcut) was defined on the host server operating system:

Shift-Control-Backspace

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 Console

To launch and use the GUI-based Oracle ILOM Remote Console for KVMS redirection, see these topics:

- "Launch and Use the Oracle ILOM Remote Console" on page 122
- "Toggle Key Sequence for Keyboard and Mouse Control" on page 124
- "Redirection Menu Options" on page 124
- "Devices Menu Options" on page 125
- "Keyboard Menu Options" on page 126
- "International Keyboard Support" on page 127

▼ Launch and Use the Oracle ILOM Remote Console

Before You Begin

- Ensure that the requirements for first-time use have been met: TABLE: Requirements for Using Oracle ILOM Remote Console on page 116.

- The Console (c) role is required to launch and use Oracle ILOM Remote Console.
- Upon launching the Oracle ILOM Remote Console, video and serial redirection options are presented only for SPARC server SPs. The Oracle ILOM Remote Console automatically launches video redirection for x86 server SPs.
- To control the use of the keyboard and mouse between the Oracle ILOM Remote Console and the host desktop, see "Toggle Key Sequence for Keyboard and Mouse Control" on page 124.
- Upon establishing the 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 Console, do the following.**

   a. **In the Oracle ILOM web interface, click Remote Console > Redirection.**

   b. **In the Launch Redirection page, click a redirection option if 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-up, 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 – Alternatively, SP and CMM users can launch the Oracle ILOM Remote Console from the Actions Panel on the Oracle ILOM web interface Summary page.

---

2. **To stop, restart, or start a new redirection session, click the Redirection menu and select the appropriate menu option.**

   For a description of menu options, see "Redirection Menu Options" on page 124.

   Special Considerations:

   - A single redirection view automatically appears when the KVMS session is launched from a single host server SP.
   - Multiple redirection views are possible when: (1) a new KVMS session is manually added; or (2) when the initial KVMS session is launched from the CMM (chassis) web interface. A CMM KVMS session presents a single redirection view for each chassis-managed CPU blade server SP.

3. **To redirect devices, click the Devices menu and select the appropriate menu option.**

   For a description of menu options, see "Devices Menu Options" on page 125

   Special Considerations:

   - If you are installing software from a distribution media (CD/DVD), ensure that the media is inserted in the local client redirected drive.
   - 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.

- For Oracle Solaris client users, you 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 privilege to the processor that is running the Oracle ILOM Remote Console by entering these commands:

    ```
    su to root
    ppriv -s +file_dac_read pid_javarconsole
    ```

4. **To set keyboard modes and send options, click the Keyboard menu and select the appropriate menu option.**

   For a description of menu options, see "Keyboard Menu Options" on page 126.

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

Toggle Key Sequence for Keyboard and Mouse Control

Use one of the following toggle key sequences to control the use of the keyboard and mouse between the Oracle ILOM Remote Console application and the local client desktop.

Local Client Device	Toggle Key Sequence
Mouse	Alt-m
Keyboard	Alt-k

Redirection Menu Options

Redirection Menu Option	Description
Start Redirection (default)	Click Start Redirection to enable redirection service. This option is enabled by default; therefore, the redirection service is automatically started when launching the Oracle ILOM Remote Console dialog.
Restart Redirection	The Restart Redirection option stops and starts the active keyboard, video, mouse, and storage redirection.

Redirection Menu Option	Description
Stop Redirection	The Stop Redirection option stops the active keyboard, video, mouse, and storage redirection.
New Session	Adds a new redirection session to the current tab set.
Delete Session	Deletes a redirection session from the current tab set.

Devices Menu Options

Devices Menu Option	Description
Keyboard (enabled by default)	Click Keyboard to toggle on or 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 toggle on or 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 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 SPARC host servers.
Save as host defaults	Click Save as host defaults to set the current Devices menu options that are selected as the defaults settings.

Keyboard Menu Options

Note – The Oracle ILOM Remote Console supports the use of all characters on the following international keyboards: Swedish, Swiss-French, and Finnish.

Keyboard Menu Option	Description
Auto-Keybreak Mode (enabled by default)	Click Auto-Keybreak Mode to automatically send a key break after every keystroke. This option can be helpful to resolve keyboard problems over slow network connections.
Stateful Key Locking	Option applies to Oracle Solaris with XSun or OSX. Click Stateful Key Locking if 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. Click Left Alt Key to toggle the left Alt key on or off.
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 enabled, 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 x86 host servers BIOS functionality.
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 with Russian and Greek keyboards.

International Keyboard Support

The Oracle ILOM Remote Console supports the use of the following international keyboard language layouts:

- Brazilian-Portuguese
- Chinese
- Chinese -Traditional (Taiwan)
- English (US)
- Estonian
- French
- German
- Italian (IT)
- Japanese
- Korean
- Spannish
- Japan (JP)
- Russian
- Turkish

First Time Setup for Oracle ILOM Storage Redirection CLI

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

The following requirements must be met prior to using the Oracle ILOM Storage Redirection CLI for the first time.

TABLE: Requirements for Using Oracle ILOM Storage Redirection

Setup Requirement	Description
JRE 1.5 environment	The storage redirection service and client are Java Web Start applications that require the installation of the Java Runtime Environment (1.5 or later) on the local client system. To download the latest Java Runtime Environment (JRE), see `http://java.com`.
Register 32-Bit JDK Plug-in and Start Storage Redirection Service	The storage redirection service must be installed locally or set to run from the Oracle ILOM web interface. The 32-bit JDK Java Plug-in must also be registered with the local client web browser. **Related Information**: • "Register Java Plug-In for Windows IE Browser and Start Service for First Time" on page 129 • "Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser" on page 130

TABLE: Requirements for Using Oracle ILOM Storage Redirection *(Continued)*

Setup Requirement	Description
Install Storage Redirection Client	After registering the 32-bit JDK plug-in with the local client web browser and starting the storage redirection service for the first-time, the storage redirection client must be installed on the local client system. **Related Information**: • "Install the Storage Redirection Client" on page 131
User Roles	A Console (c) role is required in Oracle ILOM to launch and use the Oracle ILOM Storage Redirection CLI.
Communication TCP/IP Port Required	The Oracle ILOM Storage Redirection CLI, by default, uses TCP/IP port: 2121 to communicate with the host server. **Related Information**: • "Optionally Modify the Default Network Port 2121 for Storage Redirection" on page 132

▼ Register Java Plug-In for Windows IE Browser and Start Service for First Time

Perform this procedure to: (1) register the 32-bit JDK Java plug-in with the Microsoft Windows IE browser, and (2) to start the storage redirection service for the first time:.

1. **On the local Windows client, open Windows Explorer (not Internet Explorer).**
2. **In the Windows Explorer dialog box, click Tools > Folder Options, and then click the Files Types tab.**
3. **In the Files Types tab, do the following:**
   a. **In the Registered File Type list, select the JNLP file type and click Change.**
   b. **In the Open With dialog box, click Browse to select the 32-bit JDK file stored on the local client system.**
   c. **Enable the check box for "Always use the selected program to open this kind of file."**
   d. **Click OK.**
4. **To start the storage redirection service for 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" and choose the `javaws` (default) 32-bit JDK file on the local system, and then click OK. A security warning dialog box appears prior to running the Storage Redirection service.

Special Considerations:

- If you chose 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 chose to run the `Jnlpgenerator-cli` file, and you also chose to enable the check box for "*Always perform this action when handling this file type*," the `Jnlpgenerator-cli` dialog box will become unavailable in the future to modify the default storage network port. Therefore, if in the future the default network port (2121) needs to be modified, you should not enable this check box.

6. **Start the storage redirection service by performing one of the following:**
   - **Run Service** – In the Security dialog box, click Run (or Yes) to start the service.
   - **Start service from command window or terminal** – 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 storage redirection service fails to start, an error message appears informing you of an error condition. Otherwise, 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 Console > Redirection > Launch Service.

   A dialog box appears for opening the `jnlpgenerator-cli` file.

2. **In the Opening Jnlpgenerator-cli dialog, 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" and choose the `javaws` (default) 32-bit JDK file on the local system, and then click OK. A security warning dialog box appears prior to running the Storage Redirection service.

Special Considerations:

- If you chose 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 chose to run the `Jnlpgenerator-cli` file, and you also chose to enable the check box for "*Always perform this action when handling this file type*," the `Jnlpgenerator-cli` dialog box will become unavailable in the future to modify the default storage network port. Therefore, if in the future the default network port (2121) needs 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 configured to run:**

     In the Security dialog box, click Run (or Yes) to start the service.
   - **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 storage redirection service fails to start, an error message appears informing you of an error condition. Otherwise, if an error message did not appear, the service is started and is waiting for user input

Related Information:

- "Install the Storage Redirection Client" on page 131
- "Optionally Modify the Default Network Port 2121 for Storage Redirection" on page 132

▼ Install the Storage Redirection Client

Perform the following procedure to install the storage redirection client on the local client system.

Note – This is a one-time client installation that needs to be completed before using the Oracle ILOM Storage Redirection CLI for the first time.

Before You Begin

- The Java plug-in should be registered and storage redirection service should be started for the first time.

  For instructions, see either:

  - "Register Java Plug-In for Windows IE Browser and Start Service for First Time" on page 129
  - "Start Service For First Time and Register Java Plug-In for Mozilla Firefox Browser" on page 130.

To install storage redirection client, perform these steps:

1. **In the Oracle ILOM web interface, click Remote Console > Redirection > Download Client.**

   A dialog box appears for the Opening StorageRedir.jar file.

2. **In the Opening StorageRedir.jar dialog box, do the following:**
   - Click "Save it to disk," and then click OK.
   - In the Save As dialog, save the `StorageRedir.jar` file to a location on the local client system.

Related Information:

- "Optionally Modify the Default Network Port 2121 for Storage Redirection" on page 132
- "Launching and Using the Oracle ILOM Storage Redirection CLI" on page 134

▼ 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 dialog for *Opening Jnlpgenerator-cli* file 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 Console > Redirection > Launch Service.**

        The dialog for Opening Jnlpgenerator-cli file appears.

     b. **In the Opening `Jnlpgenerator-cli` dialog, click "Save to disk," and then click OK.**

     c. **In the Save As dialog, 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, then save the changes to the file.**

   File example:

```
<application-desc>
<argument>cli</argument>
<argument>2121</argument>
</application-desc>
```

   After changing the default network port 2121 and saving the changes to the locally stored `Jnlpgenerator-cli` file, the non-default port number must always be specified when starting, stopping, or viewing storage redirections from the command window or terminal.

Launching and Using the Oracle ILOM Storage Redirection CLI

To launch and use the Oracle ILOM Storage Redirection CLI, see these topics:

- "Launch the Oracle ILOM Storage Redirection CLI and Redirect Storage Devices" on page 134
- "Interactive and Non-Interactive Shell Syntax" on page 138
- "Storage Redirection Commands and Options" on page 138

▼ Launch the Oracle ILOM Storage Redirection CLI and Redirect Storage Devices

Use the following procedure to launch and use the Oracle ILOM Storage Redirection CLI console.

Before You Begin

- Ensure that the requirements for first-time use have been met: TABLE: Requirements for Using Oracle ILOM Storage Redirection on page 128.
- The Console (c) role is required to launch and use Oracle ILOM Remote Console.
- Review syntax for shell modes and the storage redirection commands:

  "Interactive and Non-Interactive Shell Syntax" on page 138

  "Storage Redirection Commands and Options" on page 138

To launch the Storage Redirection CLI console and redirect storage devices, perform these steps:

1. **To start the storage redirection service, perform one of the following:**
   - To run the storage redirection service from Oracle ILOM web interface:

     a. **In the Oracle ILOM web interface, click Remote Console > Redirection > Launch Service.**

        The dialog for Opening Jnlpgenerator-cli file appears.

     b. **In the** `Opening Jnlpgenerator-cli` **dialog, click "Open it with" and choose the javaws (default) (32-bit JDK file), and then click OK.**

     c. **In the Warning Security 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.

- To start the (installed) storage redirection service from a command window:

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, 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 Storage Redirection CLI console using an interactive shell mode, perform these steps: 1. In the command-line interface, navigate to the directory where the Storage Redirection client (`StorageRedir.jar`) is installed using the cd command. For example: **`cd`** *my_settings/storage_redirect_directory* 2. 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" on page 138

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: 1. In the command-line interface, enter the command to launch the Storage Redirection CLI (`java -jar StorageRedir.jar`) at the shell prompt ($). $ **`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 ...` 2. If the Storage Redirection CLI fails to launch, a detailed error message appears explaining the error condition. Otherwise, the Storage Redirection CLI is ready for user input. **Note -** You can launch multiple Storage Redirection CLI consoles by issuing the Storage Redirection command (`-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" on page 138 • "Storage Redirection Commands and Options" on page 138

3. **To verify that the storage redirection service is running, type the following command:**

   `test-service`

   A message appears stating whether the redirection service passed or failed.

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

   - "Storage Redirection Commands and Options" on page 138
   - "Interactive and Non-Interactive Shell Syntax" on page 138

4. **To start storage redirection, type the following `start` command followed by the sub-commands and properties for the redirection device type, path to device, remote SP user name and password, and the IP address of the remote SP.**

   For example:

Note – Commands shown in the following example should be entered as one continuous string.

`start` -r redir_type -t redir_type_path -u remote_username [-s remote_user_password] [-p non_default_storageredir_port] remote_SP_IP

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

- "Storage Redirection Commands and Options" on page 138
- "Interactive and Non-Interactive Shell Syntax" on page 138

5. **To view active storage redirection, type the `list` command followed by the sub-commands and properties for any non-default storage redirection ports and the IP addresses of the remote host server SP.**

   For example:

   `list` [-p non_default _storageredir_port] remote_SP

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

   - "Storage Redirection Commands and Options" on page 138
   - "Interactive and Non-Interactive Shell Syntax" on page 138

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 the 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] remote_SP

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

   - "Storage Redirection Commands and Options" on page 138
   - "Interactive and Non-Interactive Shell Syntax" on page 138

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] [-p storageredir_port] remote_SP stop -r
redir_type -u remote_username [-s remote_user_password] [-p
storageredir_port] remote_SP
stop-service [-p storageredir_port]
test-service [-p storageredir_port]
help
version
quit
```

Interactive and Non-Interactive Shell Syntax

The syntax required for entering the Storage Redirection commands in either of these modes is as follows:

- **Interactive shell mode syntax**

  `storageredir` <*command*> <*command_options*> <*sub_commands*> <*sub_command_options*>

- **Non-interactive shell mode syntax**

  `$ java -jar StorageRedir.jar` <*command*> <*command_options*> <*sub_commands*> <*sub_command_options*>

Storage Redirection Commands and Options

- TABLE: Storage Redirection Commands on page 138
- TABLE: Storage Redirection Command Options on page 138
- TABLE: Storage Redirection Sub-Commands on page 139
- TABLE: Storage Redirection Sub-Command Options on page 140

TABLE: 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: 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: 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 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: 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. **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. **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. **Example**: `-s` *my_password* If this password command is not specified at the command line, the system will automatically prompt you for it.
`-p` *storageredir_port*	The `-p` *storageredir_port* identifies the Storage Redirection communication port on the local host. The default port provided is 2121. **Example:** `-p 2121`

Starting and Stopping a Host Serial Redirection Session

In addition to the Oracle ILOM Remote Console and the Storage Redirection CLI, Oracle ILOM provides the ability to launch a text-based serial redirection session to the host server operating system.

Console (c) role users in Oracle ILOM can start or stop a host serial redirection console from the CLI. After starting the redirection session, host user credentials for accessing the host operating system are required. Prior to stopping the redirection session from Oracle ILOM, host users should log out of the host operating system.

For further instructions for starting and stopping a host serial console redirection session, see the following procedures:

▼ 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.
- 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 serial redirection sessions can only be started from an Oracle ILOM SP CLI.

1. **To start a host serial redirection console from the Oracle ILOM SP CLI, type:**

   ```
   start /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, log out of the host server operating system, and then press these keys to terminate the host serial console session: `ESC` and `(`.**

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

Related Information

- "Host Serial Console Log Properties" on page 142

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 table:

TABLE: Host Serial Console Log Properties

User Interface Configurable Target and User Role:

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

Property	Default	Description
`logging`	enabled	*enabled* | *disabled* Set the `logging` property to turn on or turn off serial console history logging. If the logging property is set to disabled, the `show /HOST/console/history` command will return the following error: `failed. could not get console history` **CLI Syntax for `logging`:** **`set /HOST/console logging=`***enabled* | *disabled*
`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`:** **`set /HOST/console line_count=`***0 to 2048*

TABLE: Host Serial Console Log Properties *(Continued)*

User Interface Configurable Target and User Role:

- **SP CLI:** `/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
`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`**:** **`set /HOST/console start_from=`***beginning* | *end*
`escapechars`	#.	Specify the escape characters used to exit the console redirection session. **CLI Syntax for** `escapechars`**:** **`set /HOST/console escapechars=`***characters* **Note -** The `escapechars` property is only available for SPARC systems.

Configuring Host Server Management Actions

Description	Links
Refer to this section for descriptions of CMM and SP configurable properties for host power control.	• "Controlling Host Power to Server or Blade System Chassis" on page 146
Refer to this section for descriptions of SP configurable diagnostic properties.	• "Setting Host Diagnostic Tests to Run" on page 147
Refer to this section for descriptions of x86 SP configurable properties for next boot device.	• "Setting Next Boot Device on x86 Host Server" on page 150
Refer to this section for descriptions of SPARC SP properties for host control.	• "Setting Boot Behavior on SPARC Host Server" on page 153
Refer to this section for descriptions of SPARC SP configurable boot mode properties for OpenBoot and LDoms.	• "Overriding SPARC Host Boot Mode" on page 155
Refer to this section for descriptions of SPARC SP configurable boot properties for host domain, as well as a list of LDom configurations currently set.	• "Managing SPARC Host Domains" on page 159
Refer to this section for descriptions of SPARC SP configurable property values for the host KeySwitch state.	• "Setting SPARC Host KeySwitch State" on page 161
Refer to this section for descriptions of SPARC SP configurable property values for the host TPM state.	• "Setting SPARC Host TPM State" on page 162

Related Information

- "Maintaining x86 BIOS Configuration Parameters" on page 209

Controlling Host Power to Server or Blade System Chassis

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

System administrators can issue power control commands from the Oracle ILOM CLI or web interface. For more details about each power control command, see the following table.

TABLE: Remote Power Control Commands for Host Managed Devices

User Interface Configurable Target and User Role:

- **CLI**: <*command*> `/System`
- **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 managed 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 or blade system chassis	Use Immediate Power Off to directly shut down the power to the managed device.
Graceful Shutdown and Power Off	• `stop /System`	• Any managed server or blade system chassis	Use Graceful Shutdown and Power Off to gracefully shut down the host operating system prior to shutting down the power to the managed device.
Power On	• `start /System`	• Any managed server or blade system chassis	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

- *Oracle ILOM 3.1 User's Guide*, "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide*, "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Setting Host Diagnostic Tests to Run

Oracle ILOM provides a set of server-specific diagnostic properties that enable system administrators to control whether system diagnostic tests are run at startup.These diagnostic properties are configurable from either the Oracle ILOM CLI or web interface. For further information about these properties, see the following tables:

- TABLE: x86 Server SP Diagnostic Properties on page 147
- TABLE: SPARC Server SP Diagnostic Properties on page 148

TABLE: x86 Server SP Diagnostic Properties

User Interface Configurable Target and User Role:

- **SP CLI:** `/HOST`
- **Web**: Host Management > Diagnostics
- **User Role**: Reset and Host Control (r) role (required to modify diagnostic properties).

Requirement:

- To apply diagnostic property modifications in the web interface, you must click Save.

Property	Default	Description
Run Diagnostics on Boot (diag state=*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 state=`***disabled* | *enabled* | *extended* | *manual*

TABLE: x86 Server SP Diagnostic Properties *(Continued)*

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
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: SPARC Server SP Diagnostic Properties

User Interface Configurable Target and User Role:

- **SP CLI:** `/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, aPower-On-Self Test (POST) is run after any error-invoked power reset occurs. **CLI Syntax for Trigger:** **`set /HOST/diag/trigger=`** *error-reset* | *hw-change* | *power-on-resets*

TABLE: SPARC Server SP Diagnostic Properties *(Continued)*

User Interface Configurable Target and User Role:

- **SP CLI:** `/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 Levels (`power_on_level=` `|hw_change_level=` `|errror_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:** **`set /HOST/diag/error_reset_level=`***min* | *max* **`hw_change_level=`***min* | *max* **`power_on_level=`***min* | *max*

Trigger Verbosity
(`power_on_verbosity=`
`|hw_change_verbosity=`
`|error_reset_verbosity`
`=`)
	Min	*Normal* | *Min* | *Max* | *Debug* | *None*
		Independently set a report level for each enabled trigger:
		• Normal – When enabled, Oracle ILOM outputs a moderate amount of debugging information to the system console. Output includes the name and results for each test run.
		• Min – When enabled, Oracle ILOM outputs a limited amount of output on the system console (default).
		• Max – When enabled, Oracle ILOM outputs debugging information for each POST step to the system console.
		• Debug – When enabled, Oracle ILOM outputs an extensive debugging information to the system console. Output includes the names of the components tested and the test results for each test run.
		• None – When enabled, Oracle ILOM disables the output of debugging information to the system console.
		CLI Syntax for Trigger Verbosity:
		`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*

TABLE: SPARC Server SP Diagnostic Properties *(Continued)*

User Interface Configurable Target and User Role:

- **SP CLI:** `/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
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*

Related Information

- *Oracle ILOM 3.1 User's Guide*, "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide*, "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

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: 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**: **`set /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**: **`set /HOST/boot_device=pxe`**
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**: **`set /HOST/boot_device=disk`**

TABLE: Set Next Boot Device Property on x86 Managed Server *(Continued)*

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
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**: **`set /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**: **`set /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**: **`set /HOST/boot_device=floppy`**
BIOS (`boot_device=bios`)	Set the BIOS property to temporarily by-pass the BIOS boot order at the next host boot and to boot the system to the BIOS Utility Setup Menu. **CLI Syntax**: **`set /HOST/boot_device=bios`**

Related Information

- *Oracle ILOM 3.1 User's Guide,* "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Setting Boot Behavior 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.

TABLE: 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`**
Auto Run On Error (`autorunonerror=false|true`)	False, disabled	*False* | *True* Set to instruct Oracle ILOM to continue booting the SPARC server upon encountering a non-fatal boot error. **CLI Syntax for Auto Run On Error**: **`set /HOST autorunonerror=`***true* | *false*

TABLE: Host Control Information and Boot Properties on SPARC Managed Server *(Continued)*

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 power on the SPARC server when the Oracle Solaris 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*
Boot Timeout (`boottimeout=`)	0, timer disabled	Integer between *0* and *36000* seconds Set a timeout value for the boot timer on the SPARC server. **CLI Syntax for Boot Timeout**: **`set /HOST boottimeout=`***0 to 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*
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*

TABLE: Host Control Information and Boot Properties on SPARC Managed Server *(Continued)*

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
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

- *Oracle ILOM 3.1 User's Guide,* "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

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: Host Boot Mode Properties for Host SPARC Server

User Interface Configurable Target and User Role:

- **SP CLI:** `/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 for Host Boot Mode State**: **`set /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 for Host Boot Mode Expiration Date**: **`show /HOST/bootmode expires`**

TABLE: Host Boot Mode Properties for Host SPARC Server *(Continued)*

User Interface Configurable Target and User Role:

- **SP CLI:** `/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 64 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 for Host Boot Mode Script**: **`set /HOST/bootmode script=`***value* Where: script does not affect the current /HOST/bootmode setting. value can be up to 64 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"`**

TABLE: Host Boot Mode Properties for Host SPARC Server *(Continued)*

User Interface Configurable Target and User Role:

- **SP CLI:** `/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
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

- *Oracle ILOM 3.1 User's Guide,* "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Managing SPARC Host Domains

Oracle ILOM provides a set of host domain properties that enable system administrators to view logical domain configurations presently set on a host SPARC server, as well as set host domain properties for auto-boot and boot guests.

The Oracle ILOM host domain properties are viewable and configurable from the Oracle ILOM CLI and web interface. For more details about these properties, see the following tables:

- TABLE: View Logical Domain Configurations Detected for Host SPARC Server on page 159
- TABLE: Host Domain Configurable Properties for Host SPARC Server on page 160

TABLE: 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: 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, Oracle ILOM automatically reboots the control domain after the next power-on or 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 server power-on or reset. **CLI Syntax for Host Domain Auto-Run**: **`set /HOST/domain/control auto-boot=`***enabled* | *disabled*
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. **CLI Syntax for Host Domain Boot Guests**: **`set /HOST/domain/control boot_guests=`** *enabled* | *disabled*

Related Information

- *Oracle ILOM 3.1 User's Guide,* "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

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: 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**: **`set /SYS keyswtich_state=`***normal* | *standby* | *diag* | *locked*

Related Information

- *Oracle ILOM 3.1 User's Guide*, "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide*, "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

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 table.

Note – TPM properties for x86 servers are managed in the BIOS Utility. For further details about x86 operating system TPM properties and requirements, refer to the Oracle x86 server administration guide.

TABLE: TPM Property Values for Host SPARC Server

User Interface Configurable Target and User Role:

- **SP CLI:** `/HOST/tpm`
- **Web**: Host Management > TPM > TPM Settings
- **User Role:** Reset and Host Control (r) role (required to modify TPM property).

Requirements:

- The host SPARC server must be running an Oracle Solaris Operating System version that supports TPM.
- To apply TPM property modifications in the web interface, you must click Save.

Property	Default	Description
TPM (`activate= enable= forceclear=`)	Disabled	*Active* | *Enable* | *Forceclear* • Enable (TPM state) – This option must be enabled (set to true) in Oracle ILOM to apply TPM configuration modifications. • Activate – This option and the Enable option must be enabled (set to true) in Oracle ILOM to active the TPM configuration. • Forceclear – This option and the Enable option must be disabled (set to false) to purge the TPM state upon the next power reset. **CLI Syntax for KeySwitch**: **`set /tpm activate=`***false* | *true* **`enable=`***false* | *clear* **`forceclear=`***false* | *enable*

Related Information

- *Oracle ILOM 3.1 User's Guide*, "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide*, "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Setting Up Alert Notifications and Syslog Server for Event Logging

Description	Links
Refer to this section for information about configuring, testing, and disabling alert notifications.	• "Configuring Alert Notifications" on page 164
Refer to this section for information about configuring a Syslog server to log Oracle ILOM events to a remote host.	• "Configuring Syslog for Event Logging" on page 169

Related Information

- *Oracle ILOM 3.1 User's Guide,* "Managing Oracle ILOM Log Entries" on page 45
- *Oracle ILOM 3.1 Protocol Management Reference Guide,* "Managing SNMP Trap Alerts Using the Oracle ILOM" on page 16
- TABLE: SNMP Configuration Properties on page 84

Configuring Alert Notifications

System administrators can configure alert notifications in Oracle ILOM to provide advance warnings of possible system failures. Oracle ILOM supports the configuration of IPMI PET alerts, SNMP Trap alerts, and Email alert notifications.

Up to 15 alert notifications are configurable in Oracle ILOM using the Oracle ILOM CLI, Oracle ILOM web interface, or an SNMP client. For each configured alert notification, system administrators can optionally generate a test message to ensure that the destination recipient successfully receives the test message.

For further information about configuring alert notifications in Oracle ILOM, see the following topics:

- "Alert Notification Configuration Properties" on page 164
- "Configure and Test Alert Notification (IPMI PET, SNMP, or Email)" on page 166
- "Disable Alert Notification (IPMI PET, SNMP, or Email)" on page 168
- "Configure SMTP Client for Email Alerts" on page 168

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: 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** – Required property includes: alert destination IP address, alert destination port number, and an alert level. Each specified destination must support the receipt of SNMP Trap messages. • **Email Alerts** – Required properties include: destination email address and alert level. Prior to enabling Email alerts, properties for the SMTP email server must be configured in Oracle ILOM. **Related Information**: • *Oracle ILOM 3.1 Protocol Management Reference Guide,* "Configuring SMTP Client for Email Alert Notifications (SNMP)" on page 81
Alert Destination	Mandatory	The Alert Destination property specifies where to send the alert message. IP address destinations must be configured for IPMI PET and SNMP alerts. Email address destinations must be configured for Email alerts.
Alert Destination Port	Optional	The TCP/UDP destination port only applies to SNMP alert configurations. Oracle ILOM automatically selects a standard TCP/UDP destination port number. System administrators can optionally choose to accept the standard (162) port number or manually specify a TCP/UDP port number.
Alert Level	Mandatory	All alert notification configurations require setting an alert level. Alert levels enable the sending of the alert notification. In addition, for IPMI PET alerts and Email alerts, alert levels act as a filter mechanism to ensure alert recipients only receive the alert messages that they are most interested in receiving. 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. • **Disabled** – 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*, or *Critical*.

TABLE: Alert Notification Configuration Properties *(Continued)*

Property	Requirement	Description
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 (““).
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. For instructions for configuring and testing alert notifications from an SNMP application client, see the “Manage Component Information and Email Alerts (SNMP)” on page 73.

Before You Begin

- For Email alert configurations, the SMTP server must be configured. If the SMTP server is not configured, Oracle ILOM will not be able to generate Email alerts. For configuration details, see "Configure SMTP Client for Email Alerts" on page 168.
- For SNMP alert configurations, the property for SNMP sets must be enabled and at least one user account must be configured for SNMP. For configuration details, see TABLE: SNMP Configuration Properties on page 84.
- Admin (a) role is required in Oracle ILOM to configure alert notification properties.

1. **To populate the properties for one of the 15 alert configuration IDs, do the following:**
   - Web:

     Click ILOM Administration > Notifications > Alerts, click an Alert ID, and then click Edit. Define the required properties (level, type, and destination) and then click Save.

     For required and optional property details, see TABLE: Alert Notification Configuration Properties on page 165.
   - CLI:

     Type the following to set the required alert properties:

     set /*SP* | *CMM***/alertmgmt/rules/***n* **type=***email* | *snmptrap* | *ipmipet* **destination=***ip_address* **port=***required_for_snmptrap* **level=** *minor* | *major* | *crticial* | *disable*

     For required and optional property details, see TABLE: Alert Notification Configuration Properties on page 165.
2. **To test the configuration of an alert notification, do the following:**
   - Web:

     Click ILOM Administration > Notifications > Alerts, click a configured Alert ID, and then click Test Rule.

     A successful or failed status message appears.
   - CLI:

     Type the following to test a configured alert notification:

     set /*SP* | *CMM***/alertmgmt/rules/***n* **testalert=true**

     A successful or failed status message appears.

Related Information:

- TABLE: Alert Notification Configuration Properties on page 165
- "Configure SMTP Client for Email Alerts" on page 168
- TABLE: SNMP Configuration Properties on page 84
- *Oracle ILOM 3.1 User's Guide*, "Managing Oracle ILOM Log Entries" on page 45

- *Oracle ILOM 3.1 Protocol Management Reference Guide,* "Managing SNMP Trap Alerts Using the Oracle ILOM" on page 16

▼ 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 disabling a configured alert notification from an SNMP application client, see the "Manage Component Information and Email Alerts (SNMP)" on page 73.

Before You Begin

- Admin (a) role is required in Oracle ILOM to modify alert notification properties.

- **To disable the configuration of an alert notification, do the following:**
  - Web:

    Click ILOM Administration > Notifications > Alerts, click a configured Alert ID, and then click Edit. In the Level list box, click Disable, and then click Save.

    A successful or failed status message appears.
  - CLI:

    Type the following to disable a configured alert notification:

    `set /`*SP*|*CMM*`/alertmgmt/rules/`*n* **`level=disable`**

    A successful or failed status message appears.

▼ Configure SMTP Client for Email Alerts

The following procedure describes how to configure Oracle ILOM as an SMTP client using the Oracle ILOM CLI and web interface. Oracle ILOM must act as an SMTP client to successfully send email alert notifications.

Before You Begin

- Prior to configuring Oracle ILOM as an SMTP client, determine the IP address and port number for the outgoing SMTP email server that will process the email notifications.
- The SMTP Client property for Custom Sender is optional. This property enables Oracle ILOM to override the 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|CMM*`/clients/smtp state=enable address=`***`smtp_server_ip`**
    `port=`*smtp_server_port* **`custom_send=`***optional_string*

Related Information:

- "Configure and Test Alert Notification (IPMI PET, SNMP, or Email)" on page 166

Configuring Syslog for Event Logging

Syslog is a protocol service used for logging events to a remote log host. System administrators can enable the Syslog service in Oracle ILOM by configuring a Syslog server IP address.

The events logged to a Syslog server provide all the same information that you would see in the local Oracle ILOM event log, including class, type, severity, and description. Oracle ILOM provides properties for configuring up to two Syslog servers.

▼ Configure Syslog IP Address for Event Logging

Before You Begin

- Admin (a) role is required in Oracle ILOM to modify syslog properties.

- **To populate the IP address in one of the two Syslog properties, do the following:**
  - Web:

    Click ILOM Administration > Notifications > Syslog.

    Type the IP address for the Syslog server in the Server 1 or Server 2 text box, and then click Save.

- CLI:

  Type:

  `set /`*SP*|*CMM*`/clients/syslog destination_ip=`*syslog_server_ip*

Related Information:

- *Oracle ILOM 3.1 User's Guide,* "Managing Oracle ILOM Log Entries" on page 45

Setting System Management Power Source Policies

Description	Links
Refer to this section for descriptions of system management policies that are configurable from the server SP.	• "Power-On and Cooling-Down Policies Configurable From the Server SP" on page 172
Refer to this section for descriptions of the system management policies that are configurable from the CMM.	• "System Management Power Supply Policies Configurable From CMM" on page 174

Related Information

- "Setting Power Alert Notifications and Managing System Power Usage" on page 177

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.

TABLE: 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. **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. **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: Configurable Server SP Power-On and Cooling-Down Policies *(Continued)*

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* Enable this policy on an Oracle x86 server to satisfy the cooler operating temperature requirements for certain x86 server PCIe cards. The PCIe cool-down policy mode, when enabled, directs Oracle ILOM to lower the chassis output temperature sensor thresholds that are used by chassis fan algorithm to keep the PCIe cards operating within their required temperature range. **CLI Syntax for Set Enhanced PCIe Cooling Mode:** **set /SP/policy ENHANCED_PCIE_COOLING_MODE=** *enabled* | *disabled*
Enable a Cooldown Period Before Host Shuts Down (HOST_COOLDOWN=)	*Disabled* (default) | *Enabled* Enable this property on SPARC servers to enter a cooldown mode upon powering off the host server. The cooldown 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 for Enable Cooldown Period Before Host Shuts Down:** **set /SP/policy HOST_COOLDOWN=***enabled* | *disabled*

Related Information

- *Oracle ILOM 3.1 User's Guide*, "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide*, "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

System Management Power Supply Policies Configurable From CMM

System administrators can optionally set system management policies from the CMM to manage chassis power supply demand, power supply fan speeds, storage blade SAS-2 capability, and chassis power management.

For property descriptions of the system management policies that are configurable from the CMM, see the following table:

TABLE: Configurable CMM Power Supply Policies

User Interface Configurable Target and User Role:

- **CLI**: `/CMM/policy` - *or* - `/CH/BL`*n*`/SP/policy`
- **Web**: System Management > Policy > Policy Configuration
- **User Role:** admin (`a`) (required for all property modifications)

System Management Policy	Default	Description
Light Load Efficiency Mode (`LIGHT_LOAD_EFFICIENCY_MODE=`)	Disabled	*Disabled* | *Enabled* Enable this policy to monitor the chassis system power usage and automatically shut down the power supply unit (PSU) sides to achieve higher efficiency. **CLI Syntax for Light Load Efficiency Mode:** **`set /CMM/policy LIGHT_LOAD_EFFICIENCY_MODE=`***enabled* | *disabled*
Monitor Power Supply 0 Side 0 for power (`MONITOR_PS0_SIDE0=`)	Enabled	*Disabled* | *Enabled* Enable this policy to enable monitoring of Power Supply 0 Side 0 under Light Load Efficiency Mode. **CLI Syntax for Monitor Power Supply 0 Side 0:** **`set /CMM/policy MONITOR_PS0_SIDE0=`** *enabled* | *disabled*
Monitor Power Supply 0 Side 1 for power (`MONITOR_PS0_SIDE1=`)	Enabled	*Disabled* | *Enabled* Enable this policy to enable monitoring of Power Supply 0 Side 1 under Light Load Efficiency Mode. **CLI Syntax for Monitor Power Supply 0 Side 1:** **`set /CMM/policy MONITOR_PS0_SIDE1=`** *enabled* | *disabled*

TABLE: Configurable CMM Power Supply Policies *(Continued)*

User Interface Configurable Target and User Role:

- **CLI**: `/CMM/policy` - *or* - `/CH/BLn/SP/policy`
- **Web**: System Management > Policy > Policy Configuration
- **User Role:** admin (`a`) (required for all property modifications)

System Management Policy	Default	Description
Monitor Power Supply 1 Side 0 for power (`MONITOR_PS1_SIDE0=`)	Enabled	*Disabled* | *Enabled* Enable this policy to enable monitoring of Power Supply 1 Side 0 under Light Load Efficiency Mode. **CLI Syntax for Monitor Power Supply 1 Side 0:** **`set /CMM/policy MONITOR_PS1_SIDE0=`** *enabled* | *disabled*
Monitor Power Supply 1 Side 1 for power (`MONITOR_PS1_SIDE1=`)	Enabled	*Disabled* | *Enabled* Enable this policy to enable monitoring of Power Supply 1 Side 1 under Light Load Efficiency Mode. **CLI Syntax for Monitor Power Supply 1 Side 1:** **`set /CMM/policy MONITOR_PS1_SIDE1=`** *enabled* | *disabled*
Sun Cooling Door Installed (`COOLING_DOOR_INSTALLED=`)	Disabled	*Disabled* | *Enabled* Enable this policy to support a cooling door installed on a Sun Blade 6048 chassis. **CLI Syntax for Cooling Door Installed:** **`set /CMM/policy COOLING_DOOR_INSTALLED=`** *enabled* | *disabled*
Force Power Supply Fans to High Speed (`PS_FANS_HIGH=`)	Disabled	*Disabled* | *Enabled* Enable this policy to force the power supply fans to 100% capacity. **CLI Syntax for Force Power Supply Fans to High Speed:** **`set /CMM/policy PS_FANS_HIGH=`***enabled* | *disabled*
Force Power Supply Fans to Low Speed (`PS_FANS_LOW=`)	Disabled	*Disabled* | *Enabled* Enable this policy to force the power supply fans to 80% capacity. **CLI Syntax for Force Power Supply Fans to Low Speed:** **`set /CMM/policy PS_FANS_LOW=`***enabled* | *disabled*

TABLE: Configurable CMM Power Supply Policies *(Continued)*

User Interface Configurable Target and User Role:

- **CLI**: `/CMM/policy` - *or* - `/CH/BLn/SP/policy`
- **Web**: System Management > Policy > Policy Configuration
- **User Role:** admin (a) (required for all property modifications)

System Management Policy	Default	Description
Force Server Blade to be SAS2 Capable at 3Gbps. (FORCE_SAS2_3GBPS=)	Disabled	*Disabled* | *Enabled* Enable this policy to force the NEM(s) to run the SAS link at a slower rate, for those rare cases when this action is necessary. **CLI Syntax for Force Server Blade to be SAS2 Capable at 3Gbps:** **set /CH/BL*n*/SP/policy FORCE_SAS2_3GBPS=** *enabled* | *disabled*
Manage chassis power. **Caution -** Disabling may lead to chassis shutdown. (POWER_MANAGEMENT=)	Enabled	*Disabled* | *Enabled* Enable this policy to determine whether there is enough power in the chassis to power on a new server module installed in the chassis. **CLI Syntax for Manage Chassis Power:** **Caution -** Disabling may lead to chassis shutdown. **set /CMM/policy POWER_MANAGEMENT=** *enabled* | *disabled*

Related Information

- *Oracle ILOM 3.1 User's Guide,* "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Setting Power Alert Notifications and Managing System Power Usage

Description	Links
Refer to this section for descriptions of CMM and SP configurable properties for power consumption alert notifications.	• "Setting Power Consumption Alert Notifications" on page 178
Refer to these sections for descriptions of CMM and SP configurable properties for managing system power usage.	• "Setting CMM Power Grant and SP Power Limit Properties" on page 180 • "Setting SP Advanced Power Capping Policy to Enforce Power Limit" on page 183 • "Setting SP Power Management Settings for Power Policy (SPARC)" on page 185 • "Setting the CMM Power Supply Redundancy Policy" on page 187

Related Information

- *Oracle ILOM 3.1 User's Guide*, "Real-Time Power Monitoring Through Oracle ILOM Interfaces" on page 79
- *Oracle ILOM 3.1 Protocol Management Reference Guide*, "Manage SPARC Diagnostics, POST, and Boot Mode Operations (SNMP)" on page 101
- "Setting Up Alert Notifications and Syslog Server for Event Logging" on page 163

Setting Power Consumption Alert Notifications

Oracle ILOM provides configuration properties for power consumption alert notifications. When the configuration properties are enabled, configured email recipients receive alert notifications when the system power exceeds the set threshold(s).

Power consumption thresholds and Email alert notifications are configurable from the Oracle ILOM CLI or web interface.

For details about configuring an email alert notification, see "Configuring Alert Notifications" on page 164.

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

TABLE: Power Consumption Notification Threshold Configuration Properties

User Interface Configurable Target and User Role;

- **SP CLI:** /SP|CMM /powermgmt
- **Web**: Power Management > Consumption > Notification Threshold 1 | 2
- Admin (a) role (required to modify threshold properties).

Requirements:

- To apply threshold property modifications in the web interface, you must click Save.
- Email alert notification properties must be configured in Oracle ILOM.

Property	Default	Description
Notification Threshold 1 and 2 (threshold1=*n* | threshold2=*n*)	Disabled	*Disabled* | *Enabled* • Disabled – When disabled, the Notification Threshold property state and wattage property value (*0*) are disabled. • Enabled – When enabled, the Notification Threshold property state and the user-specified wattage property value are configurable. Specify a wattage threshold value between 1 and 65535. Oracle ILOM generates an alert event if the power on the system exceeds the set threshold. If an email alert recipient is configured, Oracle ILOM also generates a power consumption email alert to the configured recipient. **CLI Syntax for Power Consumption Notification Threshold** **`set /SP/CMM/powermgmt threshold1=`***<0 to 65535>* **`threshold2=`***<0 to 65535>* **Related Information:** • "Configuring Alert Notifications" on page 164 • *Oracle ILOM 3.1 User's Guide,* "Power Consumption Terminology and Properties" on page 81

Related Information

- *Oracle ILOM 3.1 User's Guide,* "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Setting CMM Power Grant and SP Power Limit Properties

Oracle ILOM provides SP and CMM configurable properties for limiting and granting power use on a managed system. These power limiting and power granting properties are configurable from the Oracle ILOM CLI and web interface as of firmware version 3.1.1 or later.

For further information about the configurable properties in Oracle ILOM for power limiting and power granting, see the following procedures.

- "Set CMM Blade Slot Grant Limit Property" on page 180
- "Set SP Power Target Limit Properties" on page 181

▼ Set CMM Blade Slot Grant Limit Property

Before You Begin

- Oracle ILOM CMM firmware version 3.1.1 or later is required.
- The Admin (a) role is required in Oracle ILOM to modify the Blade Slot Grant limit property.
- The Blade Slot Grant Limit property controls the amount of power the CMM will permit a CPU blade server to consume. By default, the Blade Slot Grant Limit is set to 1200 watts (maximum blade slot power limit).

  System administrators can choose to accept the default blade slot grant limit (1200 watts) or modify it. However, the grant limit property must not be set less than the blade slot power wattage already granted by the CMM (granted power). Setting the Blade Slot Grant Limit to 0 prevents the installed CPU blade server from powering-on.

Note – The Blade Slot Grant Limit is ignored by installed storage blade servers. The storage blade servers are auto-powered.

This procedure provides both web and CLI CMM instructions.

- **To set the CMM blade slot grant limit property, perform one of the following Oracle ILOM interface procedures:**

Oracle ILOM Interface	Set CMM Blade Slot Grant Limit Procedure
Web	1. Click Power Management > Allocation. 2. In the Power Grants table, click the radio button adjacent to a CPU blade server, then click Edit. **Note.** Storage blade servers appear in the table as "Ignored Auto-Powered blade." The Blade Slot Grant Limit property is ignored for storage blade servers. 3. In the Edit dialog, enable one of the following Blade Slot Grant Limit options: **Slot Maximum (default,1200 watts)** – When enabled, the CMM can grant up to 1200 watts of power to the requesting CPU blade server. - or - **Custom** - When enabled, type a number for the permitted power wattage that the CMM can grant to a requesting CPU blade server. The power wattage number must not be less then the power wattage number already granted to the blade slot by the CMM (granted power). Setting the power wattage to 0 will prevent the installed CPU blade server from powering-on. 4. Click Save to apply the changes.
CLI	• Type: **`set /CMM/powermgmt/powerconf/bladeslots/BL`***n* **`grant_limit=`***watts* *Where:* **`n`** – Type the blade slot number of an installed CPU blade server. **`watts`** – Type a number for the permitted power wattage that the CMM can grant to a requesting CPU blade server. The power wattage number must not be less then the power wattage number already granted to the blade slot by the CMM (granted power). Setting the power wattage to 0 will prevent the installed CPU blade server from powering-on.

Related Information

- *Oracle ILOM 3.1 User's Guide*, "Power Consumption Terminology and Properties" on page 81
- *Oracle ILOM 3.1 User's Guide*, "Monitoring Power Allocations" on page 83
- CMM Policy for Managing Chassis Power, "System Management Power Supply Policies Configurable From CMM" on page 174
- *Oracle ILOM 3.1 User's Guide*, "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide*, "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

▼ 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" on page 183.
CLI	1. Type: **`set /SP/powermgmt/budget pendingpowerlimit=`***value* **`activation_state=enabled commitpending=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" on page 183.

Related Information

- *Oracle ILOM 3.1 User's Guide,* "Monitoring Power Allocations" on page 83
- "Setting SP Advanced Power Capping Policy to Enforce Power Limit" on page 183
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Setting SP Advanced Power Capping Policy to Enforce Power Limit

Oracle ILOM provides an Advanced Power Capping Policy on the SP that helps to enforce the system target power limit. System administrators can choose to set either a soft cap with a grace period or a hard cap to keep the peak permitted power consumption under the target power limit. In addition, system administrators can set violation actions for when the set Power Capping Policy is violated.

The Power Capping Policy properties are configurable from the Oracle ILOM CLI and Web interface as of firmware version 3.1.1 or later. For further information about how to configure the Power Capping Policy properties in Oracle ILOM, see the following procedure.

▼ Set Advanced Power Capping Policy

Before You Begin

- Oracle ILOM SP firmware version 3.1.1 or later is required.
- The Power Limit (`power_limit`) property must be set on the server prior to setting the Power Capping Policy. For details, see "Set SP Power Target Limit Properties" on page 181.
- 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.
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 "Softcap" 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* **`commitpending=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 server if the system power consumption violates the power policy.

Related Information

- *Oracle ILOM 3.1 User's Guide*, "Power Consumption Terminology and Properties" on page 81

- *Oracle ILOM 3.1 User's Guide*, "Monitoring Power Allocations" on page 83
- CMM Policy for Managing Chassis Power, "System Management Power Supply Policies Configurable From CMM" on page 174
- *Oracle ILOM 3.1 User's Guide*, "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide*, "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

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.

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: **Performance** – When enabled, all components will run at full speed and capacity. **Elastic** – When enabled, 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. 3. Click Save to apply the changes.
CLI	1. Type the following to set the Power Management Policy: **`set /SP/powermgmt policy=`***performance* | *elastic* *Where*: policy=*performance* all components will run at full speed and capacity. policy=*elastic* 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

- *Oracle ILOM 3.1 User's Guide,* "Power Consumption Terminology and Properties" on page 81
- *Oracle ILOM 3.1 User's Guide,* "Monitoring Power Allocations" on page 83
- CMM Policy for Managing Chassis Power, "System Management Power Supply Policies Configurable From CMM" on page 174
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Setting the CMM Power Supply Redundancy Policy

Oracle ILOM provides a CMM Power Supply Redundancy Policy to prevent the loss of power to blade system chassis components. The Power Supply Redundancy Policy is configurable from the Oracle ILOM CMM CLI and web interface.

For further information about configuring a Power Supply Redundancy Policy for a blade system chassis from the Oracle ILOM CMM, see the following procedure.

▼ Set CMM Power Supply Redundancy Policy

Before You Begin

- Oracle ILOM CMM firmware version 3.1.1 or later is required.
- A minimum of two power supply units (PSU) must be initially installed within the blade system chassis to support the Power Supply Redundancy Policy.

Note – The Sun Blade 6000 PSUs contain two power sides. The Sun Blade 6048 PSU contains three power sides. It is possible for system administrators to shut down one side of the PSU by enabling the system management policy for Light Load Efficiency Mode (LLEM). The LLEM supports both redundant and non-redundant PSUs.

- The Admin (a) role is required in Oracle ILOM to modify the CMM grant limit property.
- The Power Supply Redundancy Policy controls the amount of power the CMM reserves from each PSU in case of a PSU failure. The CMM Power Supply Policy is set, by default in Oracle ILOM, to reserve half the power (N+N) from each PSU. If a PSU fails within the blade chassis, the CMM allocates the reserved power from the remaining PSU to prevent a power loss to the chassis system components.

  System administrators can choose to accept the default Power Supply Redundancy Policy (N+N) or disable it.

Note – When the PSU redundancy policy is modified, the modification will affect the power wattage the CMM is permitted to allocate to the CPU blade servers. For instance, when the redundancy policy is enabled (N+N), the CMM will re-adjust the Peak Permitted power to the wattage the PSU(s) can provide minus the wattage being reserved. If the redundancy policy is disabled and a PSU fails, the CMM will reduce the wattage for the Peak Permitted system power. If the Peak Permitted system wattage is reduced below the already Allocated Power wattage, the system administrator should take steps to power off the CPU blade servers to reduce the chassis power allocation.

This procedure provides both web and CLI CMM instructions.

- **To set the CMM Power Supply Redundancy Policy, perform one of the following Oracle ILOM interface procedures:**

Oracle ILOM Interface	Set CMM PSU Redundancy Policy Procedure
Web	1. Click Power Management > Redundancy. 2. Enable one of the following power redundancy policies: **N+N (default)** – When enabled, the CMM reserves half the power from each chassis PSU for power redundancy. - or - **None** – When enabled, the redundant PSU policy configuration is disabled. 3. Click Save to apply the changes.
CLI	• Type: **`set /CMM/powermgmt redundancy=`***redundancy* | *none* *Where:* **`redundancy (default)`** – When set, the CMM reserves half the power from each chassis PSU for power redundancy. **`none`** – When set, the redundant PSU policy configuration is disabled.

Related Information

- Force CMM Power Supply Fan Speeds, "System Management Power Supply Policies Configurable From CMM" on page 174
- CMM Policy for Managing Chassis Power, "System Management Power Supply Policies Configurable From CMM" on page 174
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Redesigned 3.1 Web Interface" on page 13
- *Oracle ILOM 3.1 User's Guide,* "Navigating the Command-Line Interface (CLI) Namespace Targets" on page 22

Performing Oracle ILOM Maintenance and Configuration Management Tasks

Description	Links
Refer to this section for information about performing firmware updates for upgradable system devices.	• "Performing Firmware Updates" on page 190
Refer to this section for information about resetting the power on the SP, CMM, or blade chassis components.	• "Reset Power to Service Processor or Chassis Monitoring Module" on page 198
Refer to this section for instruction for backing up, restoring or resetting an SP or CMM Oracle ILOM configuration.	• "Backing Up, Restoring, or Resetting the Oracle ILOM Configuration" on page 199

Related Information

- *Oracle ILOM 3.1 User's Guide,* "Taking a Snapshot: Oracle ILOM SP State" on page 68

Performing Firmware Updates

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 images are available on the Oracle product download web site for the following Oracle ILOM managed devices:

- Rackmount or blade servers (x86 and SPARC) that contain a service processor (SP)
- Blade system chassis monitoring module (CMM)
- Blade system chassis network expansion modules (NEMs) that include a service processor
- Blade system chassis storage blade servers

For firmware download instructions, see "Download Product Software and Firmware" on page xii.

Preserve Oracle ILOM Configuration

When updating to a later firmware release, the Preserve Configuration option (when enabled) saves your existing Oracle ILOM configuration and restores the user-defined configuration settings after the firmware update completes. However,

when the Preserve Configuration option is not enabled, the Oracle ILOM configuration settings (including network settings) are reset to their factory default values upon completing the firmware update process.

Note – The term *configuration* refers to the settings configured in Oracle ILOM by a user. These settings can include user account settings, SP network settings, management access settings, alert configuration settings, remote management configurations, and so on.

If you are updating to a prior firmware release and Oracle ILOM detects a preserved configuration for that release, the Preserve Configuration option (when enabled) reverts to the configuration for the prior release after the update process completes.

Generally, you should not update the firmware on your system to a prior release. However, if you determine that you need to run an earlier version of the firmware on your system, you can update the firmware to any prior firmware release that is available for download.

Before You Begin the Firmware Update

Prior to updating the Oracle ILOM firmware, you should:

1. Verify that the managed server SP or CMM has network connectivity to update the firmware image.

   For example, to verify that the server SP or CMM is connected to the network, use a remote web browser client or a remote CLI ssh client to log in to the server SP or CMM. For instruction, see "Log In to the Oracle ILOM SP or CMM" on page 19.

2. Identify the Oracle ILOM firmware version that is running on the managed device (server SP, storage server, NEM SP, or CMM).

   The firmware version for all upgradable devices appears in the Firmware page in the web interface or in the `/System/Firmware` CLI target.

3. Download the firmware image for the upgradable device from the Oracle product download web site and then place the image on a local or network share or on a TFTP, FTP, HTTP or HTTPS server.

   For firmware download instructions, see "Download Product Software and Firmware" on page xii.

4. Obtain an Oracle ILOM user name and password that has Admin (a) role account privileges. You must have Admin (a) privileges to update the firmware image.

5. Notify SP or CMM users of the scheduled firmware update and ask them to close all client sessions until after the firmware update is complete.

System administrators can use a banner message to communicate this message to users. For instructions for creating and enabling a banner message at login, see TABLE: Banner Message Configuration Properties on page 92.

6. If required by the host server platform, power off the host operating system before updating the SP firmware image.

   Note that if the host server power is ON and the platform server requires the power to be OFF, click the button in the Actions panel on the Summary web page to gracefully power off the host operating system and server. Alternatively, you can gracefully power off the host operating system and server from the CLI by issuing the following command: **`stop /System`**

▼ Update the Server SP or CMM Firmware Image

System administrators can choose to start the firmware update process for upgradable devices from the web interface Actions panel, the Maintenance Firmware Upgrade page, or a CLI target.

The following procedure explains the firmware update process using the CLI and the web interface Maintenance page.

Before You Begin

- Ensure that the initial requirements for updating the SP or CMM firmware image have been met. See "Before You Begin the Firmware Update" on page 191.
- 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 reboot.

To start the firmware update process and to verify that the update process has completed successfully, follow these steps:

1. **To start the firmware update process for a server SP or CMM image, perform the following steps using one of the Oracle ILOM interfaces:**

Oracle ILOM Interface	To Start and Run Firmware Update for SP or CMM Procedure
Web	1. Click Maintenance > Firmware Upgrade. 2. Click the button for Enter Firmware Upgrade Mode, then click OK in the upgrade confirmation dialog box to proceed. The Firmware Upgrade page displays the property for uploading the firmware image. **Note** – If the firmware image has not been downloaded from the Oracle product download web site, see these instructions to download the updated image: "Download Product Software and Firmware" on page xii. 3. In the Firmware Upgrade page, perform one the following actions: Click Browse to specify the firmware image to upload, then click the Upload button. - or - Input a URL to upload the firmware image, then click the Upload button. Oracle ILOM validates the firmware image and then displays options in the Firmware Verification page. 4. In the Firmware Verification page, enable the applicable options: **Preserve Configuration** – Enable this option to save and restore the existing Oracle ILOM firmware settings after the firmware update is complete. For further details about this option, see "Preserve Oracle ILOM Configuration" on page 190. **Preserve BIOS Configuration (x86 server SPs only)** - Enable this option to save and restore existing BIOS configurations after the update process is complete. This option is not supported on all x86 servers. Therefore, if this option is not presented, Oracle ILOM restores the default BIOS settings after completing the upgrade process. **Delay BIOS Upgrade (x86 server SPs only)** – Enable this option to postpone the x86 BIOS upgrade until after the next time the system is power-cycled. 5. Click Start to start the update process. 6. Click OK to proceed through a series of prompts until the Update Status page appears. 7. The system will automatically reboot when the Update Status indicates 100%. To verify the correct firmware version is running on the server SP or CMM, see Step 2 in the procedure.

Oracle ILOM Interface	To Start and Run Firmware Update for SP or CMM Procedure
CLI	1. 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. 2. Type **`y`** to load the image file, then type **`y`** to enable the applicable options: **Preserve Configuration** – Enable this option to save and restore the existing Oracle ILOM firmware settings after the firmware update is complete. For further details about this option, see "Preserve Oracle ILOM Configuration" on page 190. **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. 3. Oracle ILOM displays a status message when the firmware process is complete.The system will automatically reboot to apply the new firmware image. To verify that the correct firmware version is running on the server SP, see Step 2 in the procedure.

2. To verify that the updated firmware version is installed, perform one of the following:

- **Web:**

  Log in to Oracle ILOM and click System Information > Firmware to view the firmware version installed.

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

- **CLI:**

  Type: **`show /System/Firmware`**

Related Information:

- "Recover From a Network Failure During Firmware Update" on page 198
- TABLE: File Transfer Methods on page 37

▼ Update Blade Chassis Component Firmware Images

The Oracle ILOM CMM provides a centralized user interface for managing firmware updates for the following upgradable blade chassis components:

- Storage blade servers
- CPU blade servers
- NEMs containing SPs

System administrators can choose to use the CMM web interface or the CLI to view chassis component firmware versions or initiate chassis component firmware updates.

The following procedure explains the process for updating a chassis component firmware image using the web interface Firmware Update page and the CLI chassis component targets for loading the firmware update.

Before You Begin

- Ensure that the initial firmware update requirements have been met. See "Before You Begin the Firmware Update" on page 191.
- 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 completes, the system will reboot.

To start the firmware update process and to verify the update process completed successfully, follow these steps:

1. **To start the firmware update process for a server SP or CMM image, perform one of the following Oracle ILOM interface procedures:**

Oracle ILOM Interface	To start and run firmware update for blade chassis component (blades or NEMS) Procedure
Web	1. In the CMM web interface, click Firmware. 2. In the table, click the radio button adjacent to the chassis component for which you want to upgrade the firmware, then click the Firmware Update option in the Actions list box. The Firmware Upgrade page displays the property for uploading the firmware image. 3. In the Firmware Upgrade page, perform one the following actions: Click Browse to specify the firmware image to upload, then click the Upload button. - or - Input a URL to upload the firmware image, then click the Upload button. Oracle ILOM validates the firmware image, and then depending on the chassis component, Oracle ILOM either displays a button to start the firmware update process or displays a choice of configuration options for CPU blade server SPs. If you are updating the firmware for a CPU blade server SP proceed to step 4, otherwise proceed to step 5. 4. (CPU blade update only) In the Firmware Verification page, enable the applicable options available for CPU blade servers: **Preserve Configuration** – Enable this option to save and restore the existing Oracle ILOM firmware settings after the firmware update is complete. For further details about this option, see "Preserve Oracle ILOM Configuration" on page 190. **Preserve BIOS Configuration (x86 server SPs only)** - Enable this option to save and restore existing BIOS configurations after the update process is complete. This option is not supported on all x86 servers. Therefore, if this option is not presented, Oracle ILOM restores the default BIOS settings after completing the upgrade process. **Delay BIOS Upgrade (x86 server SPs only)** – Enable this option to postpone the x86 BIOS upgrade until after the next time the system is power-cycled. 5. Click Start to start the update process. 6. Click OK to proceed through a series of prompts until the Update Status page appears. 7. The system will automatically reboot when the Update Status reaches 100%. To verify the correct firmware version is running on the server SP or CMM, see Step 2 in the procedure.

Oracle ILOM Interface	To start and run firmware update for blade chassis component (blades or NEMS) Procedure
CLI	1. Navigate to the blade or NEM Firmware target, for example: **`cd /System/Firmware/Other_Firmware/Firmware_#`** *Where* **`Firmware_#`** is the number assigned to the specific blade server or NEM. 2. To load the Oracle ILOM firmware image using the CLI, issue the `load -source` command followed by a path to locate the firmware image that you want to install. For example: **`load -source`** *protocol://username:password@server_ip/<path_to_image>/<image.pkg>* *Where* the *protocol* can be: *http*, *https*, *ftp*, *tftp*, *sftp*, *scp*. A message appears prompting you to load the image. 3. Type **`y`** to load the image file. Proceed to Step 4 for CPU blade firmware updates, otherwise proceed to Step 5 for storage blade or NEM firmware updates. 4. (CPU blade update only) Type **`y`** to enable the applicable update options such as: preserve SP configuration, preserve x86 BIOS settings, or delay x86 BIOS update **Note** – Not all x86 server SPs support the option to preserve the BIOS configuration settings. If the x86 BIOS option is not presented, Oracle ILOM will automatically preserve the default BIOS settings. For further information about the preserve SP configuration, see "Preserve Oracle ILOM Configuration" on page 190. 5. Oracle ILOM displays a status message when the firmware process is complete. The chassis component will automatically reboot to apply the new firmware image. To verify the correct chassis component firmware version is installed, see Step 2 in the procedure.

2. **To verify that the updated firmware version is installed, perform one of the following:**

   - **Web:**

     Log in to the Oracle ILOM CMM and click the System Information > Firmware to view the firmware version installed for each upgradable chassis component.

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

   - **CLI:**

     Type: **`show /System/Firmware/Other_Firmware/Firmware_`***n*

Related Information:

- "Recover From a Network Failure During Firmware Update" on page 198
- TABLE: File Transfer Methods on page 37

▼ Recover From a Network Failure During Firmware Update

If a network failure occurs while performing a firmware update, Oracle ILOM automatically times out the session and reboots the system. After the system reboots, follow these guidelines to recover the firmware update process.

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

Reset Power to Service Processor or Chassis Monitoring Module

On occasion the blade chassis monitoring module (CMM) or the service processor (SP) for a server or a network express module (NEM) needs to be reset to complete an upgrade, or to clear an error state. The SP and CMM reset operation is similar to resetting a PC where all active processes are terminated and the system reboots.

Resetting the power on a server SP or CMM will automatically disconnect any current Oracle ILOM sessions and render the service processor unmanageable until the reset process is complete. However, the host operating system on a server is not affected when a rackmount server SP or a CPU blade server SP is reset.

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

▼ Reset Power to Server SP, NEM SP, or CMM

Before You Begin

- Host Control and Reset (r) role is required to reset a SP or CMM.
- After clicking the web Reset button or issuing the CLI `reset` command, Oracle ILOM will automatically display a prompt to confirm the reset operation, unless a CLI `-script` option is specified (**`reset`** *[options] target*).

This procedure provides both web and CLI instructions.

- **To reset the power to an SP or CMM, perform one of the following:**

Oracle ILOM Interface	Reset Power to SP or CMM
Web	Perform one of the following: • **Server SP**: Click ILOM Administration > Maintenance > Reset SP, then click the Reset SP button. • **CMM and blade chassis components**: Click ILOM Administration > Maintenance >Reset Components. Click the radio button adjacent to the chassis component (CMM, blade, NEM), then click the Reset button.
CLI	Perform one of the following: • **Server SP**: To reset the server SP, type: **`reset /SP`** • **CMM blade chassis components**: To reset the CMM, type: **`reset /CMM`** To reset a blade SP, type: **`reset /Servers/Blades/BL`*n*`/SP`** To reset a NEM SP, type: **`reset /System/IO_Modules/NEM`*n*`/SP`**

Backing Up, Restoring, or Resetting the Oracle ILOM Configuration

The Backup and Restore properties provided in Oracle ILOM enable system administrators to copy the current Oracle ILOM configuration to a backup XML file, and restore the configuration when needed. System administrators can choose to use the backup XML configuration file to restore the settings on the present SP or CMM, or use the backup file to install the configuration settings on other CMMs or server SPs.

The Reset Default properties provided in Oracle ILOM enable system administrators to clear any user-set Oracle ILOM configuration properties and restore them to their factory default values.

System administrators can back up and restore the Oracle ILOM configuration, and reset the configuration settings to defaults from the web interface or CLI. For further information about the use of the Oracle ILOM back up, restore, or reset default features, see the following topics:

- "Using Backup, Restore, and Reset Default Operations" on page 200
- "User Role Determines the Backup or Restore Configuration Settings" on page 200

Using Backup, Restore, and Reset Default Operations

System administrators can use the operations for Backup, Restore, and Reset Defaults in the following ways:

Replicate the Oracle ILOM configuration for use on other systems.

System administrators can replicate the Oracle ILOM configuration for use on other Oracle server SPs or CMMs by following these steps:

1. 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.
2. Save the Oracle ILOM configuration to a backup XML file.
3. Edit the backup XML file to remove settings that are unique to a particular system (such as IP address).
4. Perform a restore operation to replicate the configuration onto the other Oracle server SPs or CMMs.

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:

1. Reset the Oracle ILOM configuration to defaults.
2. Restore the Oracle ILOM configuration to the last known working configuration.

User Role Determines the Backup or Restore Configuration Settings

For security reasons, the user role privileges currently assigned to the user account used to back up or restore the XML configuration file determine how much of the configuration is included in the Backup or Restore operation.

To ensure that all configuration settings in an XML file are backed up or restored, full user role privileges are required. Therefore, system administrators performing Backup and Restore operations should have the Administrator (`administrator`) profile role assigned or all of the following user roles assigned:

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

If a user account with insufficient privileges is used to perform a Backup or Restore operation, some of the configuration settings might not be backed up or restored. For each configuration property that is not backed up or restored due to the lack of user privileges, a log entry is created in the Oracle ILOM event log.

For a list of user role descriptions in Oracle ILOM, see TABLE: Privileges Granted by a User Profile on page 31. For instructions for assigning user roles, see "Configuring Local User Accounts" on page 37.

For details about viewing and filtering events logged by Oracle ILOM, see the *Oracle ILOM 3.1 User's Guide,* "Managing Oracle ILOM Log Entries" on page 45.

▼ Back Up the Oracle ILOM Configuration Settings

System administrators can save a backup copy of the Oracle ILOM configuration file that is actively running on the server SP or CMM. Upon initiating a Backup operation, all Oracle ILOM client sessions to the SP or the CMM are momentarily suspended. The suspended sessions resume to normal after the Backup operation is complete. A Backup operation typically takes two to three minutes to complete.

Before You Begin

- To perform a configuration Backup 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 Determines the Backup or Restore Configuration Settings" on page 200.

The following Oracle ILOM configuration backup procedure provides both web and CLI instructions for the SP and the CMM.

- **To back up the Oracle ILOM configuration to an XML file, perform the following steps for one of the Oracle ILOM user interfaces listed.**

Oracle ILOM User Interface	Backing Up Oracle ILOM Configuration Settings to XML File
Web	1. Click ILOM Administration > Configuration Management > Backup/Restore. 2. Click Backup in the Operations box. 3. Click the Transfer Method box to specify a method for transferring the Oracle ILOM configuration file. For property descriptions of each file transfer method, see TABLE: File Transfer Methods on page 37. 4. 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. 5. Click Run to initiate the Backup operation. When the Backup operation is executing, client sessions to the Oracle ILOM SP or the CMM are momentarily suspended. The sessions will resume to normal after the Backup operation is complete.
CLI	1. Navigate to the `config` CLI target, for example: **`cd /SP/config`** **`cd /CMM/config`** 2. 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. 3. To initiate the Backup operation, type the following command from within the `/SP/config` or `/CMM/config` directory. For example: **`set dump_uri=`** *transfer_method***`://u`***`sername: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 TABLE: File Transfer Methods on page 37. **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 or the CMM are momentarily suspended. The sessions will resume to normal after the Backup operation is complete.

Related Information:

- "Optionally Edit the Oracle ILOM Backup XML Configuration File" on page 203
- "Restore the Oracle ILOM Backup XML File" on page 206

■ "Using Backup, Restore, and Reset Default Operations" on page 200

▼ Optionally Edit the Oracle ILOM Backup XML Configuration File

Advanced users can use the backup XML file to provision other Oracle server SPs or CMMs on the network with the same Oracle ILOM configuration. Prior to using a backup XML file on another system, system administrators should edit the file to remove any information that is unique to a particular system (for example, IP address).

Example XML File:

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

```
<SP_config version="3.0">
<entry>
<entry>
<property>/SP/clock/datetime</property>
<value>Mon May 12 15:31:09 2010</value>
</entry>
.
.
.
<property>/SP/check_physical_presence</property>
<entry>
<property>/SP/config/passphrase</property>
<value encrypted="true">89541176be7c</value>
</entry>
.
.
.
<value>false</value>
<entry>
<property>/SP/network/pendingipaddress</property>
<value>1.2.3.4</value>
</entry>
.
.
.
```

```
</entry>
<entry>
<property>/SP/network/commitpending</property>
<value>true</value>
</entry>
.
.
.
<entry>
<entry>
<property>/SP/services/snmp/sets</property>
<value>enabled</value>
</entry>
.
.
.
<property>/SP/hostname</property>
<entry>
<property>/SP/users/john/role</property>
<value>aucro</value>
</entry>
<entry>
<property>/SP/users/john/password</property>
<value encrypted="true">c21f5a3df51db69fdf</value>
</entry>
</SP_config>
<value>labysystem12</value>
</entry>
<entry>
<property>/SP/system_identifier</property>
<value>SUN BLADE X8400 SERVER MODULE, ILOM v3.0.0.0,
r32722</value>
</entry>
.
.
.
```

1. **Consider the following in the example XML file:**
   - The configuration settings, with exception of the password and the passphrase, are in clear text (unencrypted).
   - The `check_physical_presence` property, which is the first configuration entry in the file, is set to `false`. The default setting is `true` so this setting represents a change to the default Oracle ILOM configuration.
   - The configuration settings for `pendingipaddress` and `commitpending` are unique to each server. These settings should be deleted before using the backup XML file for a Restore operation on a different server.

- The user account `john` is configured with the `a`, `u`, `c`, `r`, `o` roles. The default Oracle ILOM configuration does *not* have any configured user accounts so this account represents a change to the default Oracle ILOM configuration.
- The SNMP `sets` property is set to enabled. The default setting is disabled.

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

   For example:

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

```
<entry>
<property>/SP/users/john/role</property>
<value>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" on page 203
- "Restore the Oracle ILOM Backup XML File" on page 206
- "Using Backup, Restore, and Reset Default Operations" on page 200

▼ Restore the Oracle ILOM Backup XML File

System administrators can perform a Restore operation to retrieve the XML file from a remote system, parse the contents, and update the SP (or CMM) with the backed-up configuration data. Upon initiating a Restore operation, all Oracle ILOM client sessions to the restoring server SP or CMM are momentarily suspended. The suspended sessions resume to normal after the Restore operation completes. A Restore operation typically takes two to three minutes to complete.

Before You Begin

- To perform a configuration restore operation in Oracle ILOM, the Administrator (`administrator`) profile role is required or the following user roles must be assigned: Admin (`a`), User Management (`u`), Console (`c`) Reset and Host Control (`r`) and Read Only (`o`).

  For further details, see "User Role Determines the Backup or Restore Configuration Settings" on page 200.

The following Oracle ILOM configuration restore procedure provides both web and CLI instructions for the SP and the CMM.

- **To restore the backed up Oracle ILOM configuration XML file, perform the following steps for one of the Oracle ILOM user interfaces listed.**

Oracle ILOM User Interface	Restoring a Backup Copy of the Oracle ILOM Configuration Settings
Web	1. Click ILOM Administration > Configuration Management > Backup/Restore. 2. Click Restore in the Operations box. 3. Click the Transfer Method box to specify a method for transferring the Oracle ILOM configuration file. For property descriptions of each file transfer method, see TABLE: File Transfer Methods on page 37. 4. 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. 5. Click Run to initiate the Restore operation. When the Restore operation is executing, client sessions to the Oracle ILOM SP or the CMM are momentarily suspended. The sessions will resume to normal after the Restore operation is complete.
CLI	1. Navigate to the `config` CLI target, for example: **`cd /SP/config`** **`cd /CMM/config`** 2. 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 3. To initiate the Restore operation, type the following command from within the `/SP/config` or `/CMM/config` directory. 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 TABLE: File Transfer Methods on page 37. **For example:** set load_uri= scp://adminuser:userpswd@1.2.3.4/Backup/Lab9/SP123.config When the Restore operation is executing, client sessions to the Oracle ILOM SP or the CMM are momentarily suspended. The sessions will resume to normal after the Restore operation is complete.

Related Information:

- "Using Backup, Restore, and Reset Default Operations" on page 200
- "Restore the Oracle ILOM Backup XML File" on page 206
- "User Role Determines the Backup or Restore Configuration Settings" on page 200

▼ Reset the Oracle ILOM Configuration to Factory Defaults

System administrators can restore the current Oracle ILOM configuration settings on the SP or the CMM to the original factory default settings.

For a description of the possible values you can set for a Reset to Defaults operation, see the following table.

Reset Property Value	Description
All	Set the All option to reset all of the Oracle ILOM configuration data to the default settings at the next service processor reset. This action does not erase the log file entries.
Factory	Set the Factory option to reset all of the Oracle ILOM configuration data to the default settings and erase all log files at the next service processor reset.
None (default)	Set the None option for normal operation while using the current configurations. Or use the None option to cancel a pending Reset to Defaults operation (All or Factory) before the next service processor reset.

- **To perform a Reset to Defaults operation on a server SP or CMM, perform the following steps for one of the Oracle ILOM user interfaces listed.**

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

Related Information:

- "Reset Power to Service Processor or Chassis Monitoring Module" on page 198

Maintaining x86 BIOS Configuration Parameters

Description	Links
Refer to this topic to identify ways you can manage the x86 BIOS configuration.	• "BIOS Configuration Management" on page 210
Refer to these topics for information about Oracle ILOM BIOS configuration features, terminology, and properties.	• "Oracle ILOM: BIOS Configuration Features" on page 210 • "Oracle ILOM: BIOS Terminology" on page 211 • "Web and CLI: BIOS Properties" on page 211
Refer to this section for information describing how to perform BIOS configuration tasks from Oracle ILOM.	• "Performing BIOS Configuration Tasks From Oracle ILOM" on page 216

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.

Note – For instructions on how to manage the BIOS configuration from the host BIOS Setup or from the Oracle System Assistant, refer to the Oracle x86 server administration guide.

Oracle ILOM: BIOS Configuration Features

Oracle ILOM provides a set of configurable properties that help you to manage the BIOS configuration parameters on an Oracle ILOM managed x86 server. These configurable Oracle ILOM properties enable you to:

- Back up a copy of the configuration parameters in the BIOS non-volatile data store.
- Restore a copy of the backed-up configuration parameters to the BIOS non-volatile data store.
- Reset the parameters in the BIOS non-volatile data store to factory defaults.

In addition, Oracle ILOM dynamically monitors the parameters in the BIOS non-volatile data store to ensure that they are in sync with the parameters in the Oracle ILOM BIOS Configuration file. A configuration sync status, appearing in the CLI and web interface, indicates the current state of the BIOS parameters stored in the Oracle ILOM BIOS Configuration file.

Note – For advanced users who need to provision the BIOS configuration to another Oracle x86 server, see "Optionally Edit the Oracle ILOM Backup XML Configuration File" on page 203.

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 "Performing Firmware Updates" on page 190.

Oracle ILOM: BIOS Terminology

Oracle ILOM Term	Description
BIOS	The BIOS on an Oracle x86 server is the boot firmware program that controls the system from the time the host server powers on to when the operating system takes over. The BIOS stores the system's date, time, and configuration information in a battery-powered, non-volatile data store.
BIOS version	A read-only property indicating the current BIOS firmware version installed on an Oracle x86 server.
BIOS non-volatile data store	The Oracle x86 server BIOS configuration parameters that are currently stored on the non-volatile memory chip.
Oracle ILOM BIOS configuration file	A dynamically maintained XML file on the server SP that contains a list of the BIOS configuration parameters that were last retrieved from the BIOS non-volatile data store.
Backup BIOS configuration	The configurable properties in Oracle ILOM that enable you to retrieve a copy of the parameters currently set in the BIOS non-volatile data store and save them to the Oracle ILOM BIOS Configuration file on the server SP.
Restore BIOS configuration	Configurable properties in Oracle ILOM that enable you to export the parameters in the Oracle ILOM BIOS Configuration file to the BIOS non-volatile data store.
BIOS configuration parameters	Typically the BIOS configuration parameters that are copied or exported by Oracle ILOM include the values for: setup, boot list, and boot devices.

Web and CLI: BIOS Properties

- TABLE: BIOS Web Navigation and CLI Targets on page 212
- TABLE: BIOS Web and CLI Properties on page 212
- TABLE: -force Option for CLI Commands: load and dump on page 215

TABLE: BIOS Web Navigation and CLI Targets

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

TABLE: 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.
BIOS Configuration: Sync Status (`config_sync_status=`)	Read-only	*OK* | *Reboot Required* | *Internal Error*	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.

TABLE: BIOS Web and CLI Properties *(Continued)*

Property Name	Type	Value(s)	Description
BIOS Configuration: Backup (**`dump_uri=`**)	Write-only		The BIOS Configuration Backup property enables you to create a copy of the parameters in the BIOS non-volatile data store and save those parameters to a BIOS Configuration file in the ILOM file system. For instructions for backing up the BIOS configuration, see "Back Up the BIOS Configuration" on page 220.
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	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: BIOS Web and CLI Properties *(Continued)*

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. **Note -** The Cancel Restore option in the web interface is only available if: (1) you initiated a Restore operation, and (2) the host operating system on the managed Oracle x86 server has not yet been powered down or reset. For instructions for restoring the BIOS configuration, see "Restore BIOS Configuration" on page 221.

TABLE: BIOS Web and CLI Properties *(Continued)*

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

`load_uri=-force` *restore_option***`/`***transfer_method***`://`***username:password***`@`***ipaddress_or_hostname* ***`/`***directorypath***`/`***filename*
`dump_uri=-force` *transfer_method***`://`***username:password***`@`***ipaddress_or_hostname* ***`/`***directorypath***`/`***filename*

TABLE: `-force` Option for CLI Commands: `load` and `dump` *(Continued)*

Usage – You must specify the `-force` option to prevent the `load` or `dump` command from failing when: (1) a "Pending Restore" state appears for Restore Status (`restore_status=pending_restore`) or (2) when a "Reboot Needed" state appears for BIOS Configuration Sync (`config_sync_status=reboot_needed`).

Caution - An out-of-sync version of the host BIOS Configuration file is copied to the Oracle ILOM file system when: (1) a "Reboot Needed" state appears for BIOS Configuration Sync (`sync_status=reboot_needed`) and (2) the `dump_uri=-force` option is used to back up the BIOS Configuration file.

Caution - The parameters in an existing pending restore BIOS Configuration file are replaced with the parameters from the last Backup BIOS Configuration file when: (1) a "Restore Pending" state appears for Restore Status (`restore_status=restore_pending`) and (2) the `load_uri=-force` option is used to restore the parameters in the host BIOS non-volatile data store.

Performing BIOS Configuration Tasks From Oracle ILOM

Requirements for BIOS Configuration Tasks

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" on page 211 prior to performing the BIOS configuration tasks that are documented in this section.
- If the managed Oracle x86 server is new, it should be powered-on to enable the host BIOS boot process to detect the boot devices, create an initial boot order, and save these parameters to the BIOS non-volatile data store. The managed Oracle x86 server should then be powered cycled to sync the BIOS non-volatile data store with the Oracle ILOM BIOS Configuration file.
- Setting factory defaults for the `/SP` or for the `/System/BIOS` can inadvertently affect one another. For example, setting the `/SP/reset_to_defaults` to *factory* might cause Oracle ILOM to lose the settings for `/System/BIOS/reset_to_defaults`. For instructions on how to set factory defaults for the SP and BIOS configuration, follow the steps described in "Reset Factory Defaults for SP and Oracle ILOM BIOS" on page 219.

▼ View the BIOS Configuration Sync Status and Sync the Configuration Parameters

Before You Begin

- Review the "Requirements for BIOS Configuration Tasks" on page 216.

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 server.**
   - From the web interface, click Host Management > Power Control > Power Cycle.
   - From the CLI, type: **`reset /System`**

   Oracle ILOM retrieves the parameters set in the BIOS non-volatile data store, saves them to the Oracle ILOM BIOS Configuration file, and updates the state for the Configuration Sync Status.

Related Information:

- "Reset BIOS Configuration to Factory Defaults" on page 219
- "Reset Factory Defaults for SP and Oracle ILOM BIOS" on page 219
- "Back Up the BIOS Configuration" on page 220
- "Restore BIOS Configuration" on page 221

▼ Reset BIOS Configuration to Factory Defaults

Before You Begin

- Review the "Requirements for BIOS Configuration Tasks" on page 216.

- **Perform one of the following actions to reset the BIOS non-volatile data store parameters to factory defaults:**
  - From the web interface, click System Management > BIOS, then select Factory from the Reset To Defaults list box and click Save.
  - From the CLI, type: **`set /System/BIOS reset_to_defaults=factory`**

  Oracle ILOM resets the BIOS Setup parameters in the non-volatile data store to factory defaults. The Reset To Defaults value reverts to None after the factory default parameters are applied.

Related Information:

- "View the BIOS Configuration Sync Status and Sync the Configuration Parameters" on page 218
- "Reset Factory Defaults for SP and Oracle ILOM BIOS" on page 219
- "Back Up the BIOS Configuration" on page 220
- "Restore BIOS Configuration" on page 221

▼ Reset Factory Defaults for SP and Oracle ILOM BIOS

Before You Begin

- Review the "Requirements for BIOS Configuration Tasks" on page 216

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_default` 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_default=factory`**
4. **Power cycle the Oracle ILOM SP by performing one of the following:**
   - From the web interface, click Host Management > Power Control > Reset.
   - From the CLI, type: **`reset /SP`**

   Oracle ILOM resets BIOS configuration parameters to factory defaults and returns None as the Sync Status state.

Related Information:

- "View the BIOS Configuration Sync Status and Sync the Configuration Parameters" on page 218
- "Reset BIOS Configuration to Factory Defaults" on page 219
- "Back Up the BIOS Configuration" on page 220
- "Restore BIOS Configuration" on page 221

▼ Back Up the BIOS Configuration

Before You Begin

- Review the "Requirements for BIOS Configuration Tasks" on page 216.
- The Backup BIOS Configuration operation typically takes two to three minutes to complete.

Follow this procedure to back up the parameters from BIOS non-volatile data store to the Oracle ILOM BIOS Configuration file.

1. **To back up the BIOS configuration, perform one of the following:**
   - From the web interface, click System Management > BIOS, in the Backup section select an option from the Transfer Method list box, then specify the required parameters for the Transfer Method, and click Start Backup.
   - From the CLI, type:

set dump_uri *transfer_method*://*username:password*@*ipaddress_or_hostname*/*directorypath*/*filename*

Where:

- *transfer_method* appears, type either: tftp, ftp, sftp, scp, http, or https
- *username* appears, type the name of the user account for the chosen transfer method server. A username is required for scp, sftp, and ftp. A username is not required for tftp, and it is optional for http and https.
- *password* appears, type the user account password for the chosen transfer method server. A password is required for scp, sftp, and ftp. A password is not used for tftp, and it is optional for http and https.
- *ipaddress_or_hostname* appears, type the IP address or the host name for the chosen transfer method server.
- *directorypath* appears, type the file storage location on the transfer method server.
- *filename* appears, type the name assigned to the Backup Configuration file, for example: `foo.xml`.

2. **Wait while Oracle ILOM completes the BIOS Backup operation.**

   Oracle ILOM retrieves a copy of the BIOS non-volatile data store configuration file and saves it to the Oracle ILOM file system.

Related Information:

- "Web and CLI: BIOS Properties" on page 211
- TABLE: -force Option for CLI Commands: load and dump on page 215
- "View the BIOS Configuration Sync Status and Sync the Configuration Parameters" on page 218
- "Reset BIOS Configuration to Factory Defaults" on page 219
- "Reset Factory Defaults for SP and Oracle ILOM BIOS" on page 219
- "Restore BIOS Configuration" on page 221

▼ Restore BIOS Configuration

Before You Begin

- Review the "Requirements for BIOS Configuration Tasks" on page 216.
- The data in the boot device section of the Oracle ILOM Configuration file is read-only and does not affect the parameters restored to the BIOS non-volatile data store.
- The BIOS Configuration Restore operation typically takes two to three minutes to complete.

Follow this procedure to restore the parameters in the Oracle ILOM BIOS Configuration file to the BIOS non-volatile data store.

1. **To restore the BIOS configuration, perform one of the following:**
   - From the web interface, click System Management > BIOS, select a Restore Option, select a Transfer Method option, then specify the required parameters for the Transfer Method, and click Start Restore.
   - From the CLI, type:

     `set load_uri=`*restore_option***`/`***transfer_method***`://`***username:password***`@`***ipaddress_or_hostname***`/`***directorypath***`/`***filename*

     Where:

     - *restore option* appears, type either: all, config-only, or bootlist-only
     - *transfer_method* appears, type either: tftp, ftp, sftp, scp, http, or https
     - *username* appears, type the user account name for the chosen transfer method server. A user name is required for scp, sftp, and ftp. A user name is not required for tftp, and it is optional for http and https.
     - *password* appears, type the user account password for the chosen transfer method server. A password is required for scp, sftp, and ftp. A password is not used for tftp, and it is optional for http and https.
     - *ipaddress_or_hostname* appears, type the IP address or the host name for the chosen transfer method server.
     - *directorypath* appears, type the storage location for the Oracle ILOM Configuration file (`/System/BIOS/Config`) on the transfer method server.
     - *filename* appears, type the name assigned to the Oracle ILOM Configuration file, for example: `foo.xml`.

Note – To cancel a pending restore BIOS configuration action, type: `set action=cancel`

---

2. **Wait while Oracle ILOM completes the Restore operation.**

   Oracle ILOM exports the BIOS configuration parameters from the Oracle ILOM BIOS Configuration file to the BIOS non-volatile data store, and updates the state of the Restore Status.

3. **Verify the state of the Restore Status to determine whether the Restore operation succeeded.**

   For a list of Restore Status state descriptions, see the "Web and CLI: BIOS Properties" on page 211.

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

Related Information

- "Web and CLI: BIOS Properties" on page 211
- TABLE: -force Option for CLI Commands: load and dump on page 215
- "View the BIOS Configuration Sync Status and Sync the Configuration Parameters" on page 218
- "Reset BIOS Configuration to Factory Defaults" on page 219
- "Reset Factory Defaults for SP and Oracle ILOM BIOS" on page 219
- "Back Up the BIOS Configuration" on page 220

SAS Zoning Chassis Blade Storage Resources

Description	Links
Refer to this section to learn about supported management options for zoning chassis-level storage devices.	• "Zone Management for Chassis-Level SAS-2 Capable Resources" on page 226
Refer to this section for information about Oracle ILOM Sun Blade Zone Manager properties.	• "Sun Blade Zone Manager Properties" on page 227
Refer to this section for important information about saving, backing up, and recovering SAS zoning configuration parameters.	• "Important SAS Zoning Allocations Considerations" on page 236
Refer to this section for procedures for enabling the Sun Blade Zone Manager and creating SAS zoning assignments.	• "Enabling Zoning and Creating SAS-2 Zoning Assignments" on page 237
Refer to this section for procedures for viewing or modifying existing storage allocations.	• "Managing Existing SAS-2 Storage Resource Allocations" on page 251
Refer to this section for resetting all saved storage allocations to factory defaults.	• "Resetting Sun Blade Zone Manager Allocations to Factory Defaults" on page 259
Refer to this section to optionally reset the in-band management password.	• "Resetting the Zoning Password to Factory Default for Third-Party In-Band Management" on page 260

Zone Management for Chassis-Level SAS-2 Capable Resources

Oracle ILOM provides zone management support for chassis-level SAS-2 storage devices installed in a Sun blade chassis system. You can choose to manage access to the Sun blade chassis-level storage resources by using the Oracle ILOM Sun Blade Zone Manager or a third-party in-band application. For more details, see:

- "Zone Management Using a Third-Party In-Band Management Application" on page 226
- "Zone Management Using Oracle ILOM Sun Blade Zone Manager" on page 226
- "Manageable SAS-2 Zoning-Capable Devices" on page 227

Zone Management Using a Third-Party In-Band Management Application

If your environment supports managing access to chassis-level storage devices using a third-party in-band management application, you should verify that the state for the Sun Blade Zone Manger in Oracle ILOM is disabled (default). If you need to reset the in-band management password to factory defaults, you can reset this password in Oracle ILOM. For instructions, see "Resetting the Zoning Password to Factory Default for Third-Party In-Band Management" on page 260.

Zone Management Using Oracle ILOM Sun Blade Zone Manager

When the Sun Blade Zone Manager is enabled in the Oracle ILOM CMM you can manage chassis-level SAS-2 storage permissions to Sun blade CPU servers installed in the chassis. For further details about using the Oracle ILOM Sun Blade Zone Manager, see these topics:

- "Manageable SAS-2 Zoning-Capable Devices" on page 227
- "Sun Blade Zone Manager Properties" on page 227
- "Important SAS Zoning Allocations Considerations" on page 236
- "Enabling Zoning and Creating SAS-2 Zoning Assignments" on page 237
- "Managing Existing SAS-2 Storage Resource Allocations" on page 251
- "Resetting Sun Blade Zone Manager Allocations to Factory Defaults" on page 259

Manageable SAS-2 Zoning-Capable Devices

The Oracle ILOM CMM recognizes the following devices in a Sun blade chassis system as manageable SAS-2 zoning-capable devices:

- Sun blade CPU server with SAS-2 RAID expansion modules (REMs)
- Sun blade chassis system Network express modules (NEMs)
- Sun blade storage server (such as the Sun Blade Storage Module M2)

Note – Oracle ILOM does not support zoning management for: (1) internal storage modules installed on a Sun blade CPU server; (2) Fabric Expansion Modules (FMODs) on a Sun storage blade; or, (3) external network SAS-2 storage resources that are connected to a Sun blade chassis system through the external SAS-2 ports of a NEM.

Note – The Sun Blade Zone Manager CLI will not recognize or list the presence of non-manageable, non-supporting SAS-2 storage devices. However, in some instances, the Sun Blade Zone Manager web interface might recognize and list the presence of non-manageable, non-supporting SAS-2 storage devices. In these cases, the non-SAS-2 storage devices in the Sun Blade Zone Manager web interface are labeled as non-SAS-2 resources.

Sun Blade Zone Manager Properties

Oracle ILOM provides a set of easy-to-use properties for setting up and managing access permissions to chassis-level SAS-2 storage devices. For more details, see:

- "Sun Blade Zone Manager Web: Properties" on page 228
- "Sun Blade Zone Manager CLI: Targets and Properties" on page 234

Sun Blade Zone Manager Web: Properties

The Sun Blade Zone Manager Settings page is accessible from the Oracle ILOM CMM web interface by clicking System Management > SAS Zoning. The Sun Blade Zone Manager Settings page provides the following options for enabling, setting up, and managing SAS zoning permissions:

- "Sun Blade Zone Manager: State" on page 228
- "Whole Chassis Setup: Quick Setup" on page 228
- "Full Resource Control: Detailed Setup" on page 232
- "Zoning Reset: Reset All" on page 233

Sun Blade Zone Manager: State

The state for the Sun Blade Zone Manager in the Oracle ILOM CMM web interface appears on the Sun Blade Zone Manager Settings page.

When this state is enabled, the Sun Blade Zone Manager provides template-based (Quick Setup) or custom zoning capabilities (Detailed Setup) for chassis-installed SAS-2 storage devices.

When this state is disabled (default), Oracle ILOM is unable to manage the access permissions to the chassis-installed SAS-2 storage devices, and the options for Quick Setup and Detailed Setup are hidden from view on the Sun Blade Zone Manager Settings page.

For instructions for enabling the Sun Blade Zone Manager state, see "Access and Enable Sun Blade Zone Manager" on page 238.

Whole Chassis Setup: Quick Setup

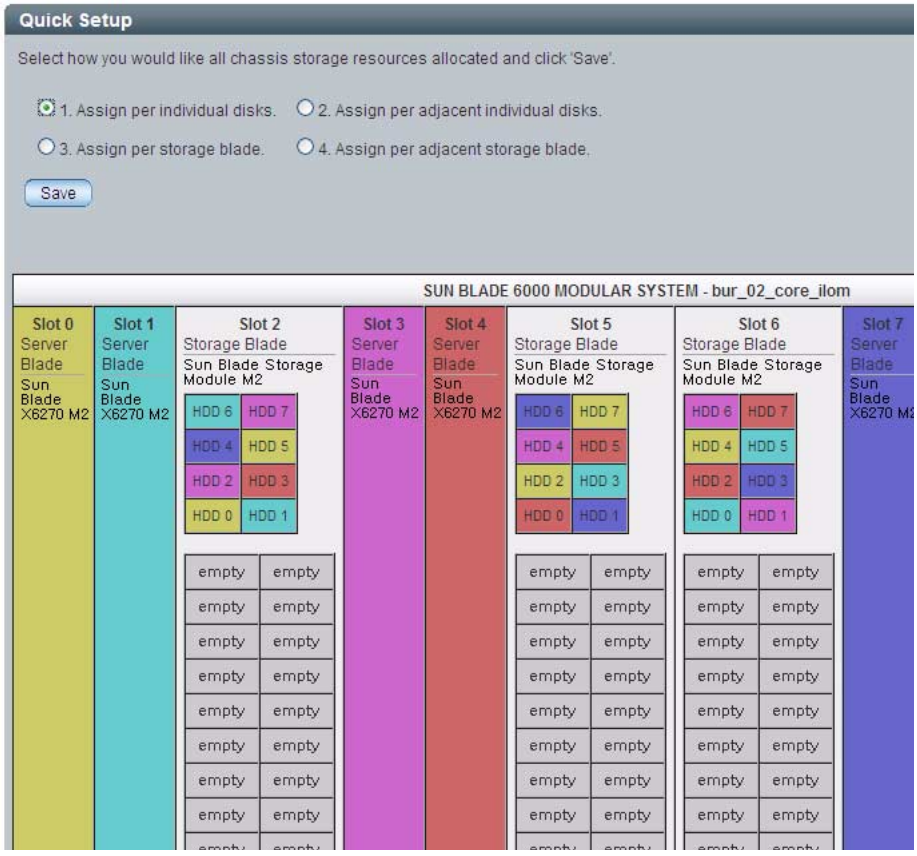
The Whole Chassis Setup feature, in the web interface, is typically used when setting up zoning access for the first time for all chassis-level SAS-2 storage devices. This feature offers the following Quick Setup zoning options:

- "Option 1: Assign to Individual Disks (Quick Setup)" on page 229
- "Option 2: Assign to Adjacent Individual Disks (Quick Setup)" on page 229
- "Option 3: Assign to Individual Storage Blade (Quick Setup)" on page 230
- "Option 4: Assign to Adjacent Storage Blade (Quick Setup)" on page 231

Option 1: Assign to Individual Disks (Quick Setup)

The first zoning option, shown in the Quick Setup dialog, uses a round-robin algorithm to evenly allocate storage ownership across all chassis CPU blade servers.

Option 1 is best suited for fault-tolerant chassis system operation where the failure or removal of a single storage blade server will not bring down all storage arrays.



Note – Empty slots shown in the Quick Setup dialog represent chassis blade slots that are empty (nothing installed).

Option 2: Assign to Adjacent Individual Disks (Quick Setup)

The second zoning allocation option, shown in the Quick Setup dialog, equally divides the number of blade storage disks among the adjacent CPU blade servers.

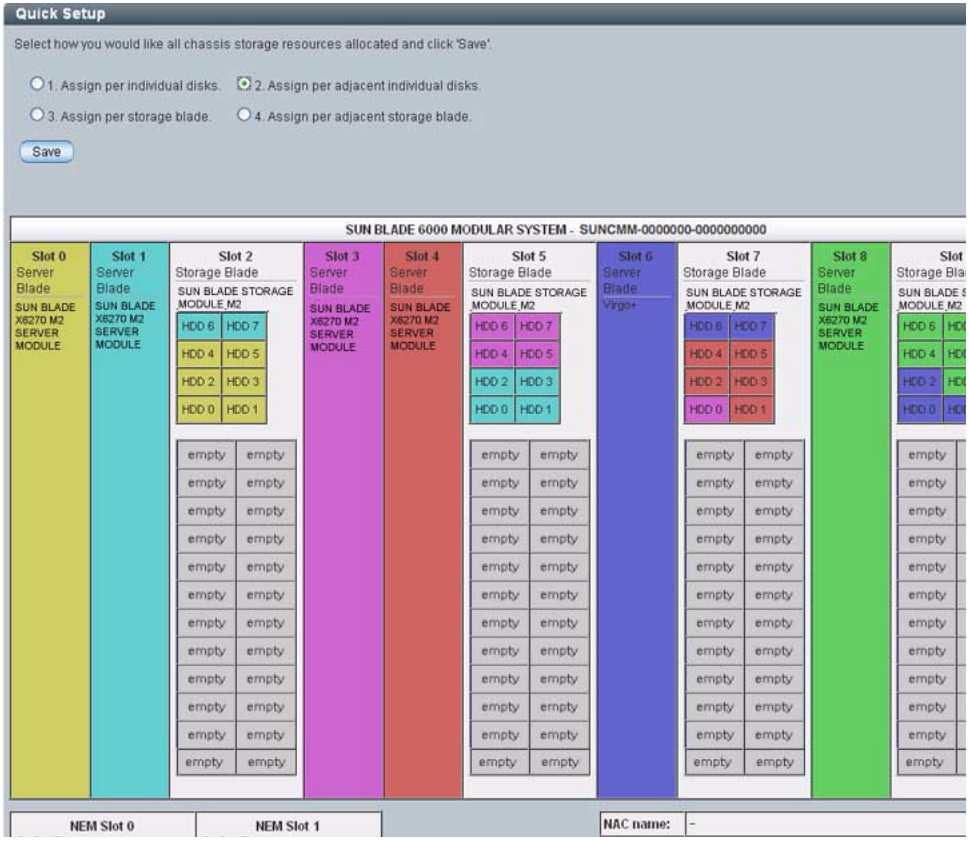
Option 2 attempts to allocate the same number of storage disks as possible to each adjacent CPU blade server. If there are no storage blades adjacent to a CPU blade, then Sun Blade Zone Manager will allocate storage disks from the nearest possible storage blade.

Assigning CPU blades to adjacent storage disks is best suited for when: 1) the Sun blade chassis system contains more CPU blade servers than storage blade servers, and 2) you want to equally deploy the storage resources among each CPU blade server.

Option 3: Assign to Individual Storage Blade (Quick Setup)

The third zoning allocation option, shown in the Quick Setup dialog, scans the Sun blade chassis system for CPU blade servers (starting at Slot 0) and then assigns the the storage disks from the closest available storage blade.

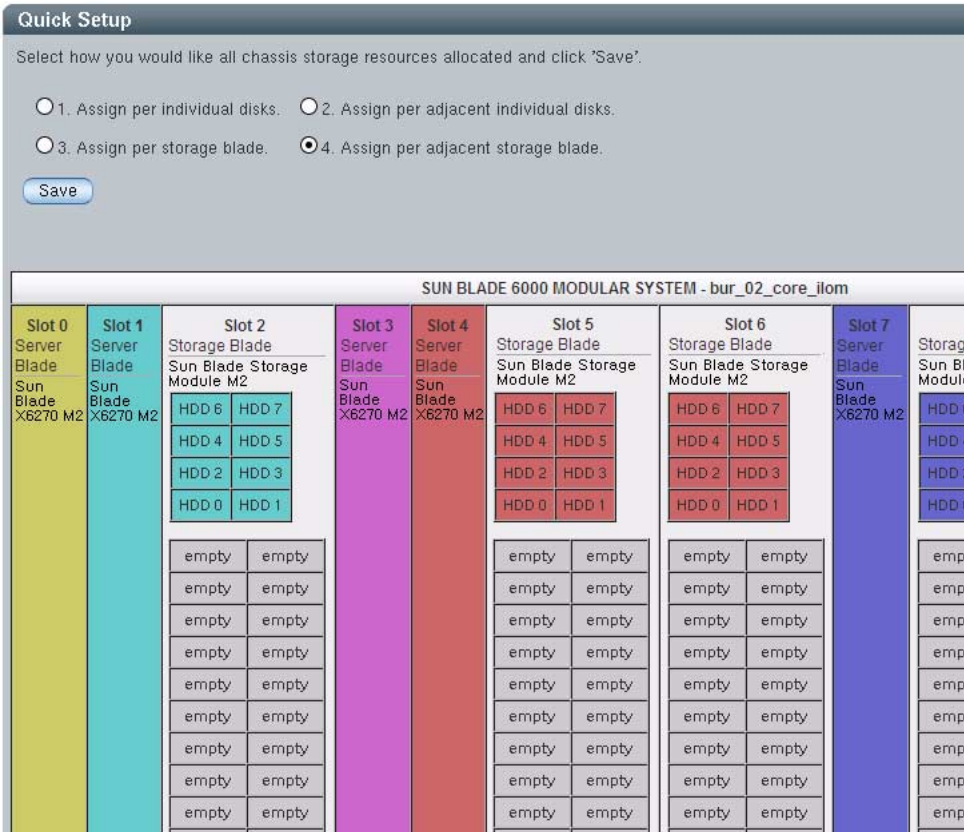
Option 3 is best suited for chassis systems that contain an equal number of storage blade servers and CPU blade servers, or there are more storage blade server than CPU blade servers. Otherwise, if there are fewer storage blade servers than CPU blade servers in the chassis, the Sun Blade Zone Manager will not be able to allocate storage to some CPU blade servers.



Option 4: Assign to Adjacent Storage Blade (Quick Setup)

The fourth zoning allocation option, shown in the Quick Setup dialog, scans the Sun blade chassis system for CPU blade servers with a storage blade in an adjacent slot. If the CPU blade server does not have a storage blade server in an adjacent chassis slot, the Sun Blade Zone Manager will not allocate storage to that CPU blade server.

Option 4 is best suited for chassis systems that contain: (1) an equal number of storage blade servers and CPU blade servers, and (2) each CPU blade server is installed in a chassis slot that is adjacent to a storage blade server.



Note – NEM0 and NEM1 targets appear in the Zone Manager when these NEMs are installed; however, external NEM connections to SAS-2 network storage devices are not supported or shown in the Sun Blade Zone Manager.

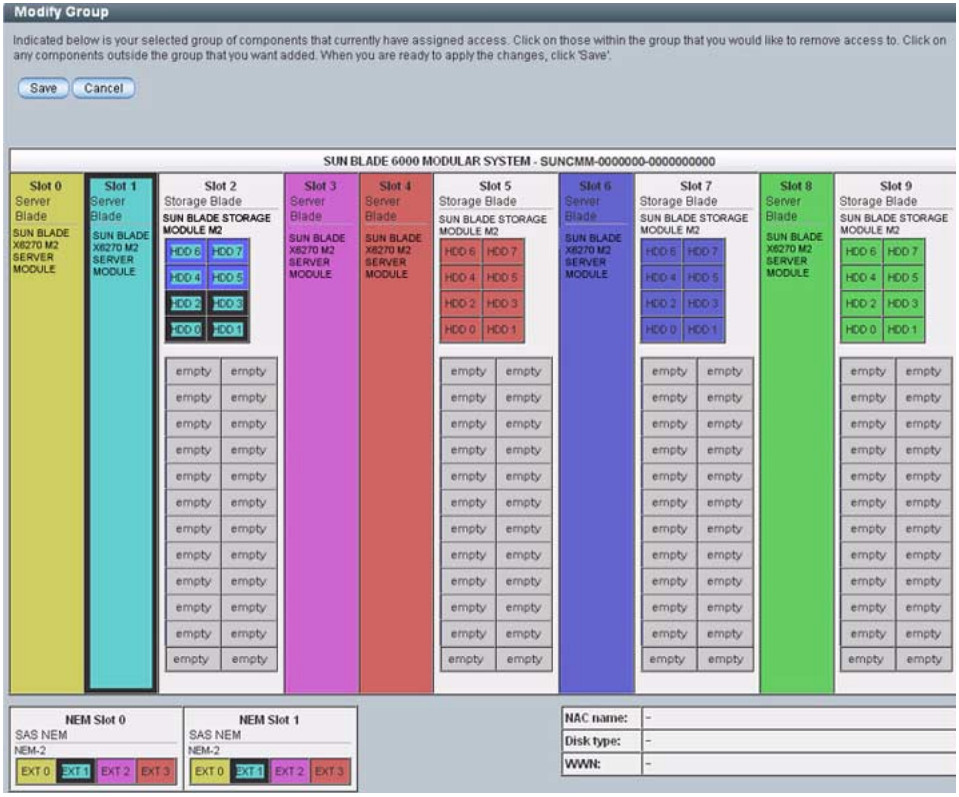
For further instructions on how to create SAS zoning allocations for the whole chassis, see "Allocating Storage to Entire Chassis: Quick Setup (Web)" on page 240.

Full Resource Control: Detailed Setup

The Full Resource Control: Detailed Setup option, in the web interface, enables you to create new allocations to storage resources or change existing storage resource allocations. For instance, when using the Full Resource Control: Detailed Setup option, you can choose to:

- Add storage allocations to a CPU blade server by clicking components outside the color-coded server group.

- Remove storage resource allocations assigned to a CPU blade server by clicking components within a color-coded server group
- Share a single resource allocation between one or more CPU blade servers.



For further instructions for using the Detailed Setup option for creating or changing resource allocations, see:

- "Allocate Storage Resources to Single Blade Server: Detailed Setup (Web)" on page 242
- "Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup (Web)" on page 245
- "Modify Existing Blade Group Allocations (Web)" on page 254

Zoning Reset: Reset All

When the state for the Sun Blade Zone Manager is enabled, the option for resetting the zoning configuration to factory defaults appears on the Sun Blade Zone Manager Settings page (System Management > SAS Zoning).

For instructions for resetting the Sun Blade Zone Manager parameters to factory defaults, see "Reset Zoning Allocations to Factory Defaults (Web)" on page 259.

Sun Blade Zone Manager CLI: Targets and Properties

The Oracle ILOM CMM CLI provides access to zoning targets and properties under the `/STORAGE/sas_zoning` namespace.

SAS Zoning Properties	Values	Default	Description
`zone_management_state=`	d*isabled* | *enabled*	Disabled	When set to disabled, the Sun Blade Zone Manager is unable to manage the SAS-2 chassis storage resources. When set to enabled, the Sun Blade Zone Manager provides template-based or custom zoning capabilities for chassis-installed SAS-2 resources.
`reset_password_action=`	*true*		When set to true, the in-band management zoning password on the CMM is set to factory defaults (all zeros).
`reset_access_action=`	*true*		When set to true, the storage resource allocation parameters currently saved on the CMM are set to factory defaults.

When zoning is enabled, blades and NEMs that are SAS-2 capable appear as CLI targets under `/STORAGE/sas_zoning`. For example:

```
-> show /STORAGE/sas_zoning

     Targets
       BL0
       BL6
       BL7
       BL8
       BL9
       NEM0
       NEM1

    Properties
      zone_management_state = enabled
      reset_password_action = (Cannot show property)
      reset_access_action = (Cannot show property)

    Commands:
```

```
cd
set
show
```

Note – NEM0 and NEM1 targets appear in the Zone Manager when these NEMs are installed; however, external SAS connections in the Sun Blade Zone Manager are not supported at this time.

SAS-2 capable storage devices on a blade server appear as targets under `sas_zoning/BL`*n*. For example:

```
-> show /STORAGE/sas_zoning/BL9

  Targets:
    HDD0
    HDD2
    HDD3
    HDD5
```

The SAS zoning properties that are available under the blade target (BL*n*) or storage device (HDD*n*) target include:

Blade and Storage Properties	SAS Zoning Target	Description
`add_storage_access=`	/BL*n*	Use the `add_storage_access=property under the /sas_zoning/BLn target` to allocate storage to a CPU blade server.
`remove_storage_access=`	/BL*n*	Use the `remove_storage_access=` property under the `/sas_zoning/BL`*n* target to remove storage from a CPU blade server.
`add_host_access=`	/BL*n*/HDD*n*	Use the `add_host_access=` property under the `/sas_zoning/BL`*n*`/HDD`*n* target to allocate storage to a CPU blade server.
`remove_host_access=`	/BL*n*/HDD*n*	Use the `remove_host_access=` property under the `/sas_zoning/BL`*n*`/HDD`*n* target to remove storage from a CPU blade server.

For further instructions on how to manage storage resource allocations from the Oracle ILOM CLI, see:

- "Manually Create SAS-2 Zoning Allocations (CLI)" on page 249
- "View and Modify Existing Storage Allocations (CLI)" on page 257
- "Reset Zoning Allocations to Factory Defaults (CLI)" on page 259

Important SAS Zoning Allocations Considerations

Saving Storage Allocations

When you save storage allocations to a blade, consider the following:

- The storage allocations saved in Oracle ILOM are based on the hardware currently installed in the chassis (SAS-2 NEMs or storage blades). Changes in the chassis hardware configuration can result in a loss of a storage blade group. Therefore, you should back up all chassis storage allocations in Oracle ILOM. For more information, see "Backing Up and Recovering SAS-2 Zoning Assignments" on page 237.

Note – Hot-plugging of chassis components such as NEMs and storage blades can also affect the storage blade group allocations. For further information on the effects of hot-plugging NEMs and storage blades, refer to the Oracle Sun storage blade or NEM hardware documentation.

- The Sun Blade Zone Manager dialog (Modify Group or New Assignments) must remain open during the entire Save operation. If the Sun Blade Zone Manager dialog is closed while the Save operation is in progress, only a portion of the storage blade group will be preserved.
- Do not remove or power cycle any of the chassis hardware components that are part of a storage blade group while a Save operation is in progress. Doing so will cause the group allocation not to save properly.

Backing Up and Recovering SAS-2 Zoning Assignments

Oracle ILOM provides Backup and Restore operations that enable you to: (1) create a backup copy of all parameters saved in the Oracle ILOM Configuration file, and (2) restore a backup copy of the Oracle ILOM Configuration file. For details about how to create a backup copy or how to restore a backup copy of the Oracle ILOM Configuration file, see "SAS Zoning Chassis Blade Storage Resources" on page 225.

Enabling Zoning and Creating SAS-2 Zoning Assignments

Chassis Hardware Requirements

- A PCIe 2.0 compliant midplane must exist in the Sun Blade 6000 chassis. For more information on determining this, refer to the *Sun Blade 6000 Modular System Product Notes*.
- The minimum software release of 3.2.1 must be installed on the CMM. This release includes the minimum Oracle ILOM CMM firmware version (3.0.10.15a), which supports SAS-2 and includes the Sun Blade Zone Manager.
- All SAS-2 storage devices (blade server module with SAS-2 REM, SAS-2 NEMs, and SAS-2 storage modules) must be properly installed and powered-on in the Sun blade chassis system.

Note – If the state of a SAS-2 storage device is in a failed state, the Sun Blade Zone Manager might not be able to recognize the failed SAS-2 storage device. For more information about identifying and resolving hardware failures using Oracle ILOM, see "Administering Open Problems" on page 41.

- SAS-2 NEMs must be at a firmware version level that supports zoning. Check your NEM product notes for version information and available updates.
- Initial setup and configuration of your Oracle ILOM CMM must be completed. For information about establishing a management connection to the Oracle ILOM CMM, see "Setting Up a Management Connection to Oracle ILOM and Logging In" on page 1.

▼ Access and Enable Sun Blade Zone Manager

When enabled, the Sun Blade Zone Manager in Oracle ILOM provides a way of constraining which CPU blade servers within a SAS domain have access to storage resources (HDDs, FMODs, external SAS ports).

Before You Begin

- The Admin (a) role is required in Oracle ILOM to modify SAS Zoning properties.
- Review "Chassis Hardware Requirements" on page 237.
- Review "Important SAS Zoning Allocations Considerations" on page 236.

Note – The presence of chassis storage blades in the Oracle ILOM web interface are not shown in the CMM Manage menu. Storage disks installed on storage blade servers are viewable from the System Information > Storage page. Sun storage blade resource allocations are manageable from the System Management > SAS Zoning > Sun Blade Zone Manager Settings page.

1. **To access and enable the Sun Blade Zone Manager from the CMM web interface, perform these steps:**

   a. **Click System Management > SAS Zoning.**

      The Sun Blade Zone Manager Settings page appears.

b. Enable SAS Zoning by selecting the Enabled check box and clicking Save.

After enabling the Sun Blade Zone Manager, you can create, view, and manage settings for SAS-2 zoning using Oracle ILOM interfaces.

The following message might appear if the Oracle ILOM CMM services are still initializing:

```
Sun Blade Zone Manager Not Ready
The Sun Blade Zone Manager is initializing and not ready for
operation. Please wait several minutes and then refresh to check
the status.
```

If the above message appears, wait five minutes and then try again. You will need to close and reopen, or refresh the web interface page.

2. To enable the SAS Zoning property from the CMM CLI, type:

```
set /STORAGE/SAS_zoning zone_management_state=enabled
```

- The following message appears.

  ```
  Enabling the Sun Blade Zone Manager will result in the
  clearing of all zoning configuration in the installed
  chassis SAS hardware, and any SAS disk I/O in progress will
  be interrupted.

  Are you sure you want to enable the Sun Blade Zone Manager
  (y/n)?
  ```

- To continue, type: **y**

  The following message appears.

  ```
  Set 'zone_management_state' to 'enabled'
  ```

- If the Oracle ILOM CMM is unable to initialize the Sun Blade Zone Manager, the following message appears:

  ```
  set: The Sun Blade Zone Manager is initializing and not
  ready for operation. Please wait several minutes and try
  again.
  ```

  If the above message appears, wait five minutes and retry the command.

Related Information

- "Allocating Storage to Entire Chassis: Quick Setup (Web)" on page 240
- "Allocate Storage Resources to Single Blade Server: Detailed Setup (Web)" on page 242
- "Manually Create SAS-2 Zoning Allocations (CLI)" on page 249
- "Managing Existing SAS-2 Storage Resource Allocations" on page 251
- "Resetting Sun Blade Zone Manager Allocations to Factory Defaults" on page 259

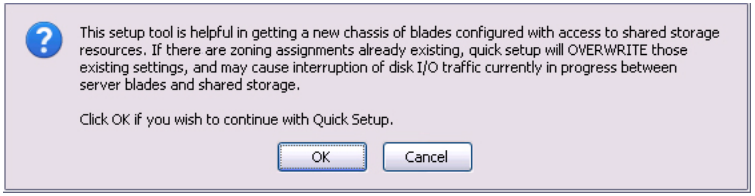
▼ Allocating Storage to Entire Chassis: Quick Setup (Web)

Before You Begin:

- The Admin (a) role is required in Oracle ILOM to modify SAS Zoning properties.
- Review "Chassis Hardware Requirements" on page 237.
- SAS Zoning must be enabled in Oracle ILOM prior to performing this Quick Setup procedure for assigning zoning. For instructions, see "Access and Enable Sun Blade Zone Manager" on page 238.

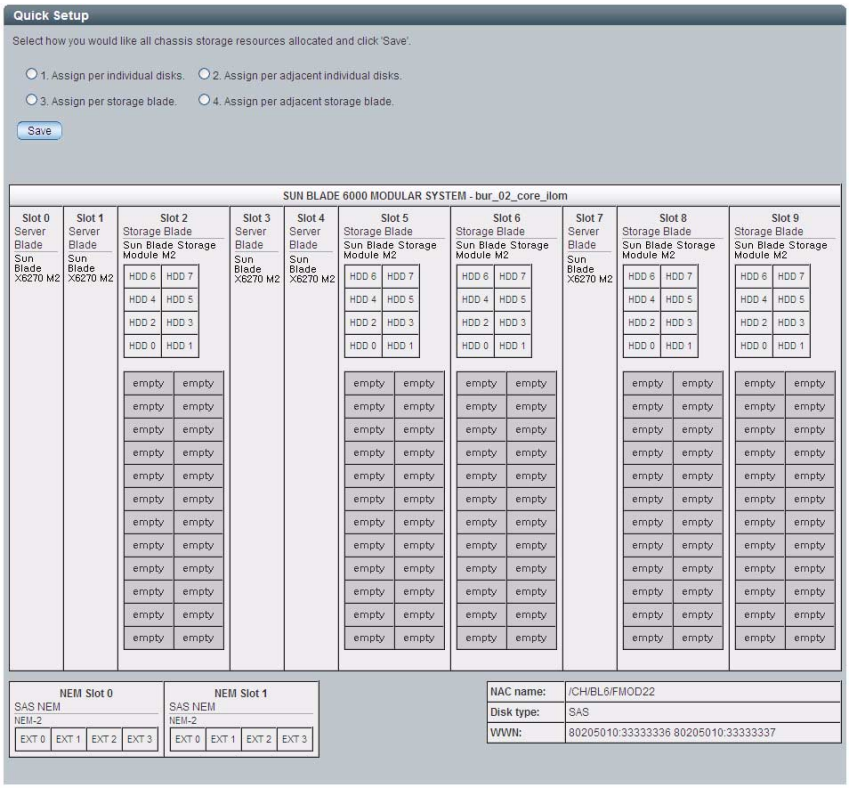
1. **To access the Sun Blade Zone Manager Settings page in the web interface, click System Management > SAS Zoning.**
2. **In the Sun Blade Zone Manager section, click the Quick Setup button.**

   A warning message appears.



3. **To overwrite existing zoning assignments, click OK.**

   The Quick Setup screen appears.



Note – Any HDD chassis slot that does not have a HDD presently installed in the chassis is labeled "empty." Empty HDD chassis slots are not included in the Quick Setup storage assignments.

---

4. **To indicate how you would like to allocate the chassis storage resources, select one of the Quick Setup options.**

   For a description of each Quick Setup option, see "Whole Chassis Setup: Quick Setup" on page 228.

   After choosing a Quick Setup option, the Sun Blade Zone Manager displays the color-coded zoning allocations between the CPU blade servers and storage devices (HDDs) installed on the storage blade servers. Although the Sun Blade Zone Manager shows the NEM0 and NEM1 External SAS connections, these connections are not supported.

Note – Until you click the Save button, the chassis storage allocations are not saved.

---

5. **To save the Quick Setup chassis storage allocations, click Save.**

6. **To back up the newly saved blade storage group allocations, see** "Backing Up and Recovering SAS-2 Zoning Assignments" on page 237**.**

Related Information

- "Important SAS Zoning Allocations Considerations" on page 236
- "Allocate Storage Resources to Single Blade Server: Detailed Setup (Web)" on page 242
- "Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup (Web)" on page 245
- "Modify Existing Blade Group Allocations (Web)" on page 254
- "Manually Create SAS-2 Zoning Allocations (CLI)" on page 249
- *Sun Blade 6000 Modular System Documentation*

▼ Allocate Storage Resources to Single Blade Server: Detailed Setup (Web)

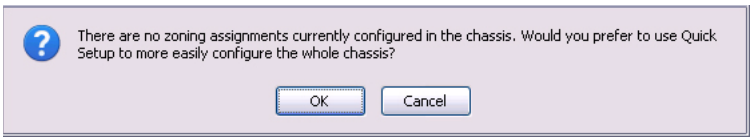
Before You Begin:

- The Admin (a) role is required in Oracle ILOM to modify SAS Zoning properties.
- Review "Chassis Hardware Requirements" on page 237.
- The Sun Blade Zone Manager must be enabled in Oracle ILOM prior to performing this procedure. For instructions, see "Access and Enable Sun Blade Zone Manager" on page 238.

1. **In the Sun Blade Zone Manager Settings page, click the Detailed Setup button.**

   One of the following appears:

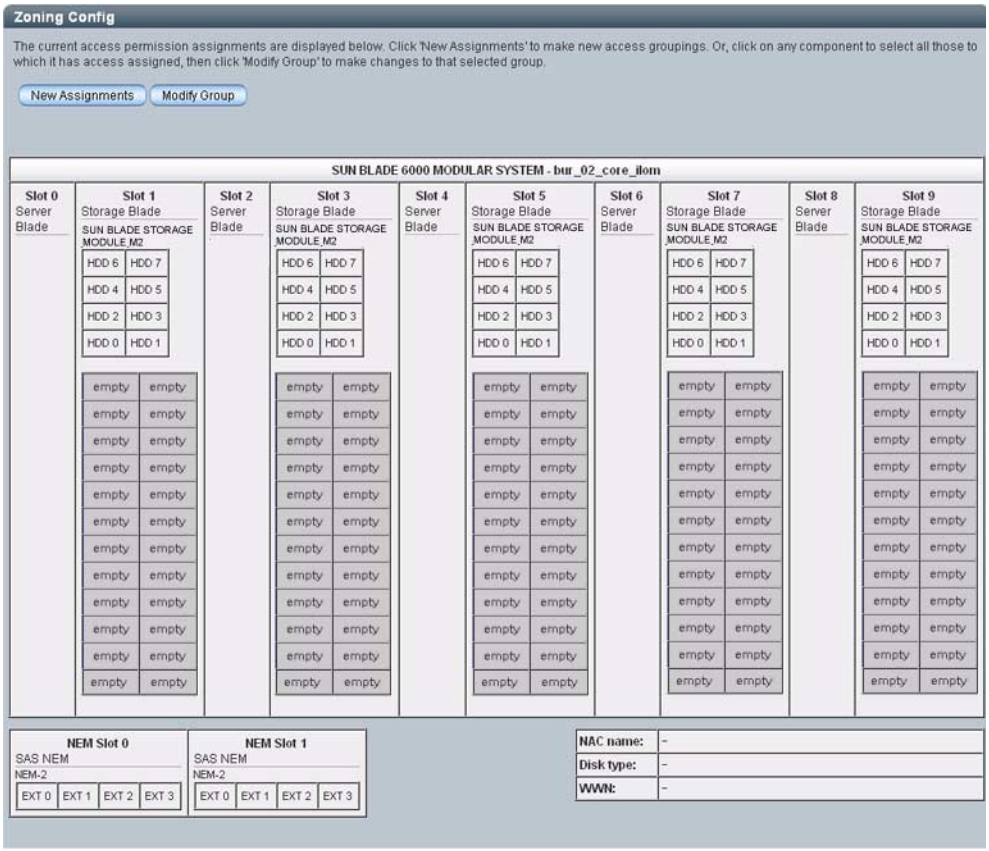
   - **The Zoning Config dialog appear**s. Proceed to Step 3.
   - The following **message appears indicating no zoning assignments exist**. Proceed to Step 2.



2. **In the message that states no zoning assignments exist, perform one of the following:**

   - If you want to manually create SAS zoning assignments using the Detailed Setup option, click Cancel and proceed to Step 4.

     Clicking Cancel will open the Detailed Setup Zoning Config page.



- If you want to set up the initial zoning assignments using Sun Blade Zone Manager Quick Setup option, click OK and proceed to "Allocating Storage to Entire Chassis: Quick Setup (Web)" on page 240.

3. **To assign storage resources to a single blade server, perform these steps in the Zoning Config dialog:**

   a. **Click New Assignments.**

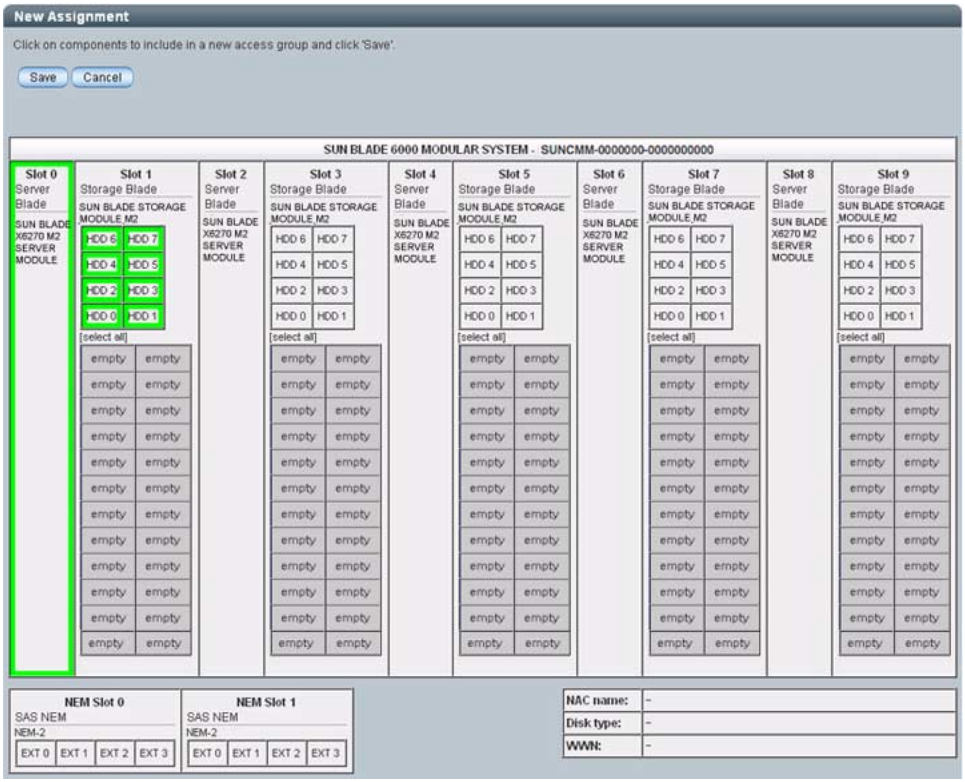
      New Assignments dialog appears.

   b. **Click a blade server then click the storage resources (HDDs) that you want to assign to the selected blade server.**

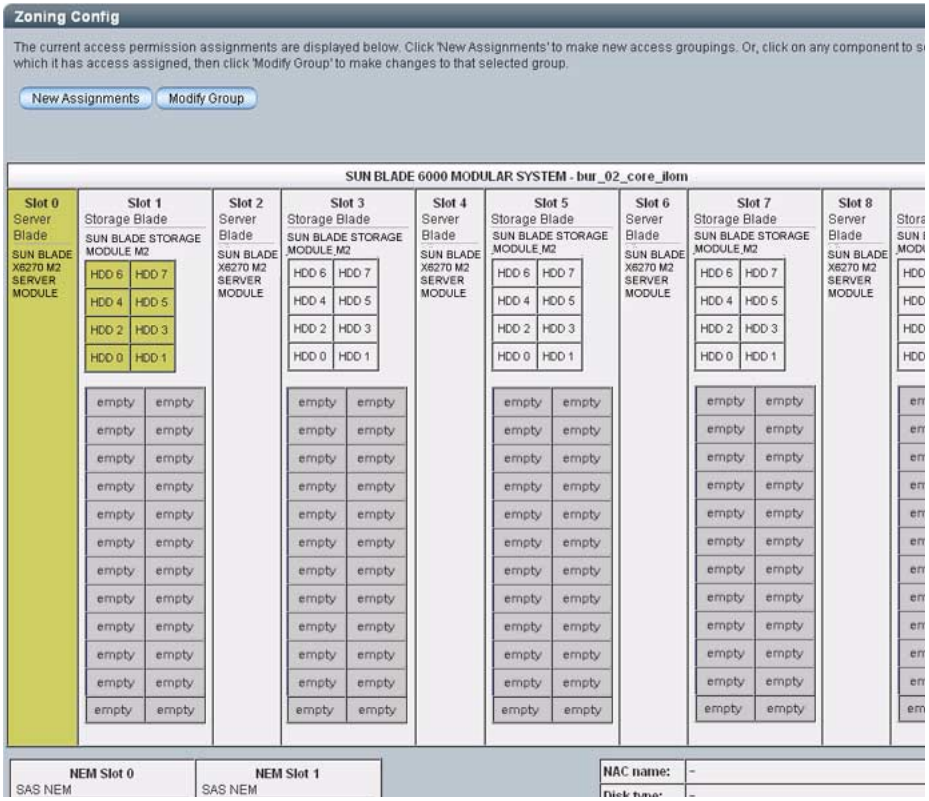
Note – All HDD chassis slots that do not have an HDD storage device installed are labeled "empty." Empty HDD chassis slots are not allocated to CPU blade servers.

Caution – Alternatively, you can allocate storage resources to multiple blade servers; however, the servers must be enabled for multipathing. For further instructions, see "Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup (Web)" on page 245.

Although the Sun Blade Zone Manager displays them, NEM0 and NEM1 External SAS connections are not supported.



c. To save the newly created blade storage group assignment, click Save.



4. **To back up the newly saved blade storage group allocations, see** "Backing Up and Recovering SAS-2 Zoning Assignments" on page 237**.**

Related Information

- "Modify Existing Blade Group Allocations (Web)" on page 254
- "Important SAS Zoning Allocations Considerations" on page 236
- "Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup (Web)" on page 245
- *Sun Blade 6000 Modular System Documentation*

▼ Allocate Single Storage Resource to Multiple Blade Servers: Detailed Setup (Web)

Before You Begin

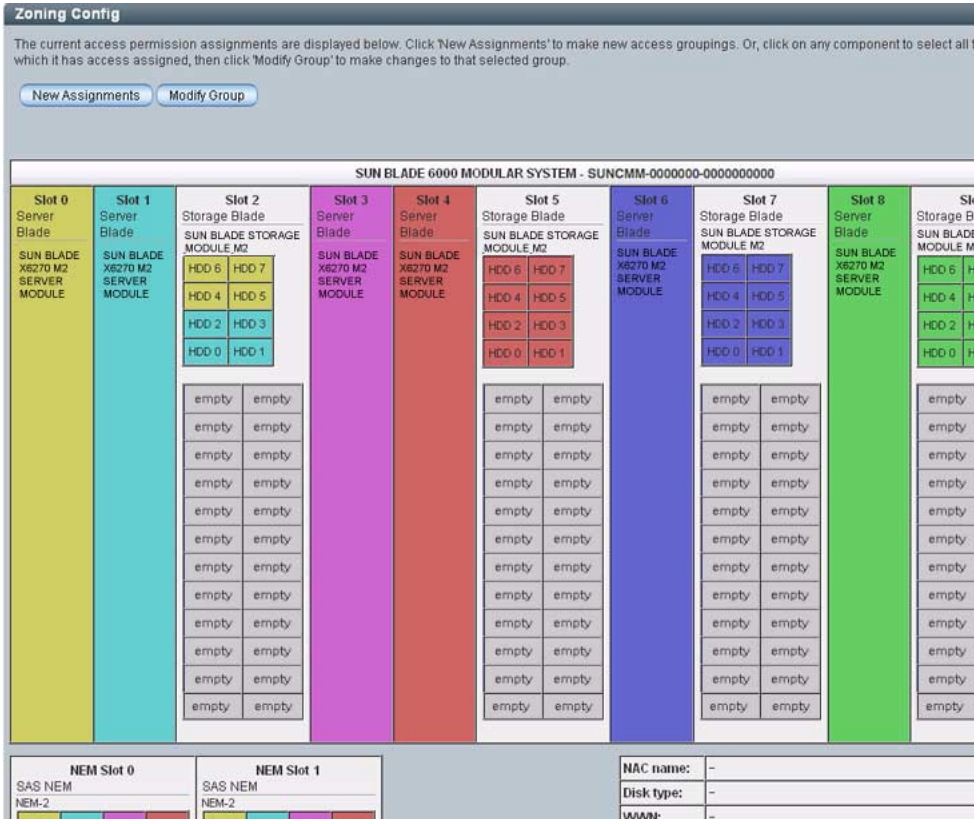
Caution – Refer to the Sun blade server documentation to determine whether the Sun blade server module is enabled for sharing storage resources with another Sun blade server module.

Caution – The option for sharing a single storage resource should only be used with an Oracle-supported clustering solution. For more information about clustering solutions, see the *Sun Blade Storage Module Administration Guide*.

- The Admin (a) role is required in Oracle ILOM to modify SAS Zoning properties.
- Review "Chassis Hardware Requirements" on page 237.
- The Sun Blade Zone Manager must be enabled in Oracle ILOM prior to performing this procedure. For instructions, see "Access and Enable Sun Blade Zone Manager" on page 238.

1. **In the Sun Blade Zone Manager Settings page, click the Detailed Setup button.**

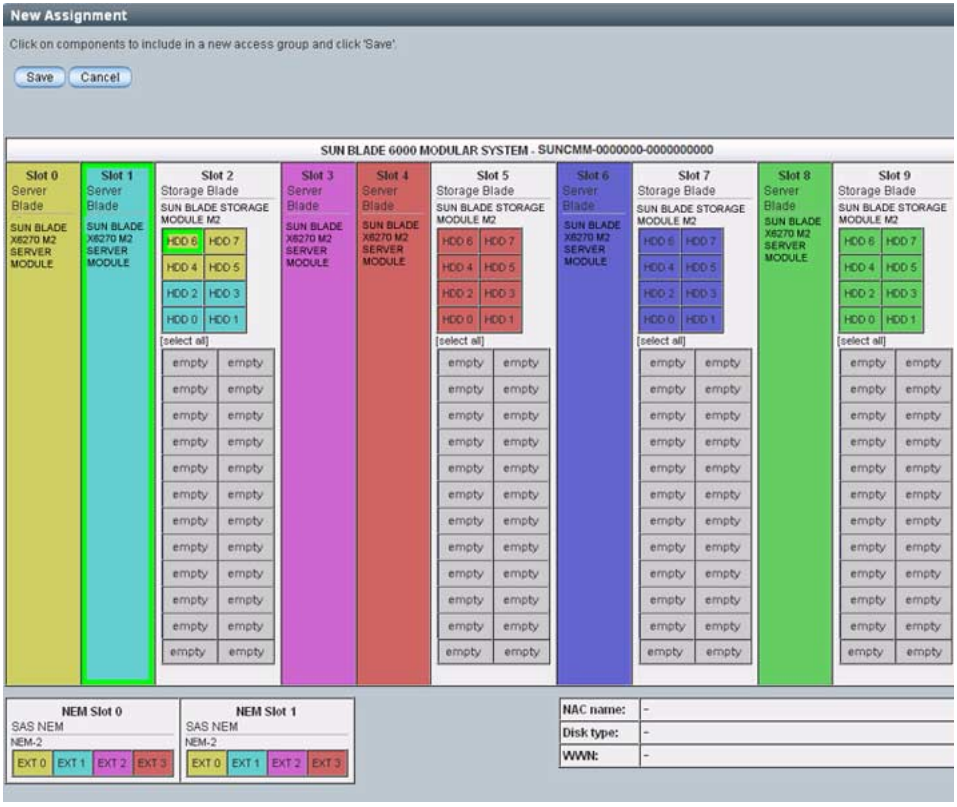
   The Zoning Config dialog appears. For example:



2. **To assign a single storage resource to multiple blade servers, perform the following steps:**

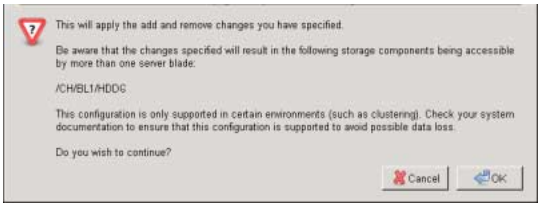
   a. **Click New Assignments.**

   b. **To share a single storage blade resource (for example, HDD6 in slot 2) currently assigned to a single blade server (for example, in slot 0) with another blade server (for example, in slot 1), click the additional blade server target (for example, in slot 1), then click the storage blade resource (for example, HDD6 in slot 2) that you want to share with this target (for example, in slot 1).**



   c. **To save the allocation modification to the blade storage group, click Save.**

   The following message appears.

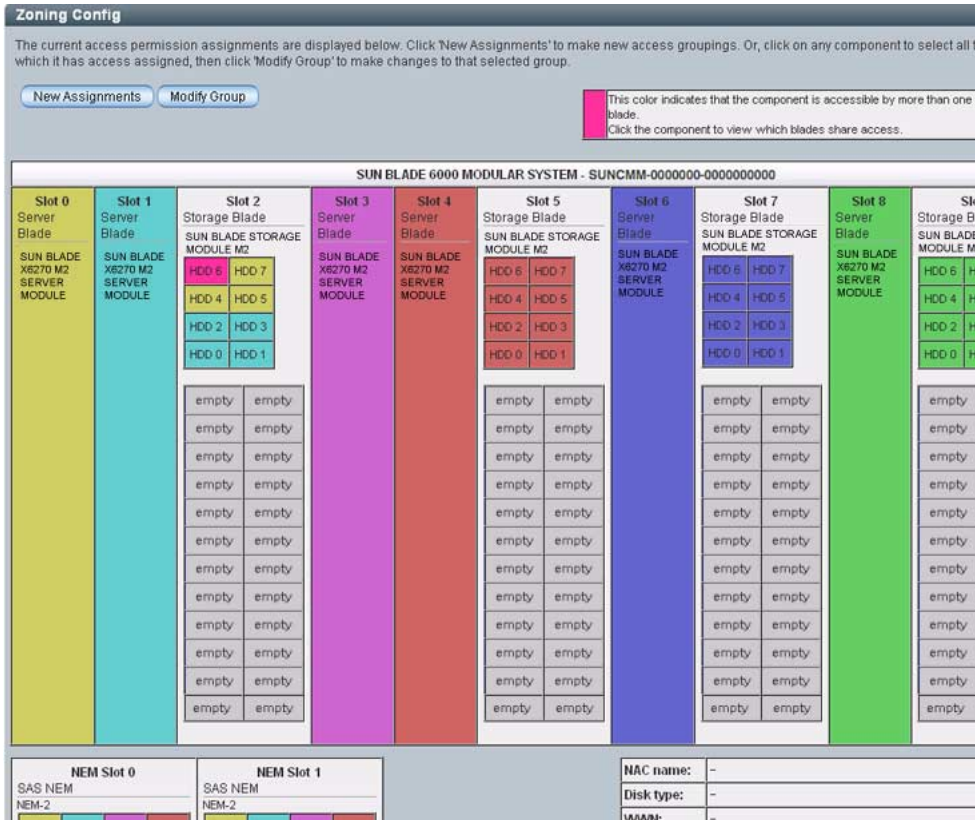


d. To continue to save the blade storage group assignment, click OK.

The Sun Blade Zone Manager highlights the shared storage resources in pink.

Example:

The HDD6 storage resource in slot 2 is highlighted with pink to indicate this resource is shared by more than one CPU blade server.



3. To back up the newly assigned blade storage group, see "Backing Up and Recovering SAS-2 Zoning Assignments" on page 237**.**

Related Information

- "Important SAS Zoning Allocations Considerations" on page 236

- "Managing Existing SAS-2 Storage Resource Allocations" on page 251
- *Sun Blade 6000 Modular System Documentation*

▼ Manually Create SAS-2 Zoning Allocations (CLI)

Before You Begin

- Ensure that your chassis configuration meets the requirements in "Chassis Hardware Requirements" on page 237.
- Admin (a) role privileges are required to manually create SAS zoning allocations in Oracle ILOM.
- The Sun Blade Zone Manager must be enabled in Oracle ILOM.

1. **Access the Sun Blade Zone Manager from the CLI.**

   For instructions, see "Access and Enable Sun Blade Zone Manager" on page 238.

2. **Use one of the following methods to allocate a storage resource to a CPU blade server:**

   - **Method 1**: To assign a storage disk to a CPU blade server, use the following commands:

     -> **cd /STORAGE/sas_zoning/BL***n*

     -> **set add_storage_access=***path_to_storage_disk*

     Where BL*n* is the chassis slot number for the CPU blade server and *path_to_storage_disk* is the path to the storage blade disk that you want to assign to the CPU blade server.

     For example, to assign the hard disk drive in the storage blade slot location 0 to the CPU blade server in chassis slot location 1, you would type:

     -> **set add_storage_access=/CH/BL1/HDD0**.

   - **Method 2**: To assign CPU blade server to a storage resource, type:

     -> **cd /STORAGE/sas_zoning/BL***n***/HDD***n*

     -> **set add_host_access=***path_to_blade_server*

     Where BL*n* is the chassis slot location for the CPU blade server, HDD*n* is storage blade slot location for the hard disk drive, and *path_to_blade_server* is the CPU blade server target where you want to assign to the storage disk.

     For example, if you wanted to assign a hard disk drive within a storage blade server to a CPU blade server in the chassis, you would type:

     -> **cd /STORAGE/sas_zoning/BL1/HDD0**

```
-> set add_host_access=/CH/BL0
```

The following examples show how to use these commands to set up zoning assignments between storage devices on a storage blade in slot 1 and a server blade in slot 0.

- **Method 1** - Command examples for allocating storage resources to a CPU blade server:

CLI Command Syntax Examples	Instructions
`-> cd /STORAGE/sas_zoning/BL0`	1. Use the first command syntax example to access the CPU blade server that will be assigned a storage resource. 2. Use the second command syntax example to allocate the storage module (HDD0) in the storage blade server (BL1) to the host CPU blade server (BL0) in chassis slot 0. 3. Optionally, you can use the third command syntax to assign multiple devices in a single command line. Ensure that you specify the full path to the storage resource and separate each resource with a comma (no space). 4. Use the `show` command to confirm that the storage allocations are saved to the CPU blade server (/CH/BL1/HD0 and CH/BL1/HDD1).
`-> set add_storage_access=/CH/BL1/HDD0`	
`-> set add_storage_access=/CH/BL1/HDD0,/CH/BL1/HDD1`	

`-> show`
`/STORAGE/sas_zoning/BL0`
`Targets:`
`0 (/CH/BL1/HDD0)`
`1 (/CH/BL1/HDD1)`	

- **Method 2** - Command examples for assigning a CPU server blade (BL0) to a storage blade resource (BL1/HDD0):

CLI Command Syntax Examples	Instructions
-> **cd /STORAGE/sas_zoning/BL1/HDD0**	1. Use the first command syntax example to access the storage resource (HDD0) installed in the storage blade server (BL1/HDD0).
-> **set add_host_access=/CH/BL0**	2. Use the second command syntax example to assign the storage resource (HDD0) to the host CPU blade server (BL0).
-> **show** /STORAGE/sas_zoning/BL1/HDD0 Targets: 0 (/CH/BL0)	3. Use the `show` command to confirm that the storage allocations are saved to the correct CPU blade server (/CH/BL0).

3. Back up the newly saved server storage group.

Related Information

- "Backing Up and Recovering SAS-2 Zoning Assignments" on page 237
- "Manually Create SAS-2 Zoning Allocations (CLI)" on page 249
- *Sun Blade 6000 Modular System Documentation*

Managing Existing SAS-2 Storage Resource Allocations

The Sun Blade Zone Manager in Oracle ILOM enables you to manage existing allocations to chassis storage resources in the following ways:

- "View Existing CPU Blade Server Storage Allocations (Web)" on page 251
- "Modify Existing Blade Group Allocations (Web)" on page 254
- "View and Modify Existing Storage Allocations (CLI)" on page 257

▼ View Existing CPU Blade Server Storage Allocations (Web)

Before You Begin

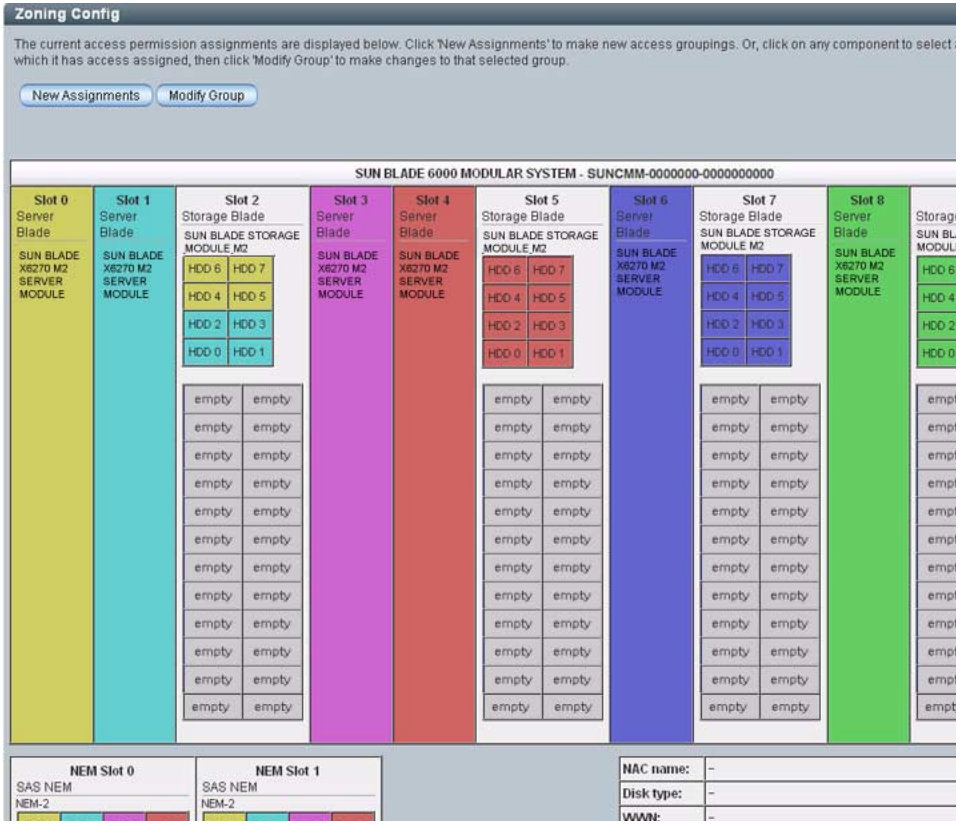
- Admin (a) role privileges are required to view Sun Blade Zone Manager allocations in Oracle ILOM.

- The Sun Blade Zone Manager in Oracle ILOM must be enabled.

1. **Access the Sun Blade Zone Manager and click Detailed Setup.**

   For instructions for accessing the Sun Blade Zone Manager, see "Access and Enable Sun Blade Zone Manager" on page 238.

   The Zoning Config dialog appears displaying the current chassis storage allocations.



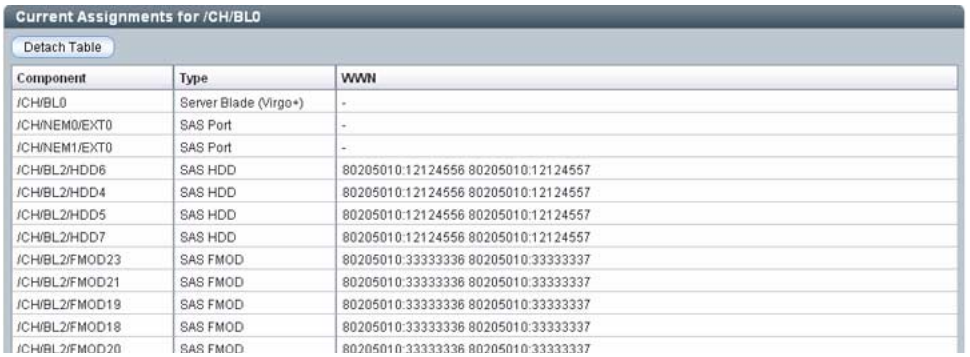
2. **To view all of the resource allocations for a selected CPU blade server, perform these steps:**

   a. **Select a CPU blade server slot.**

      For this example, slot 0 is selected.

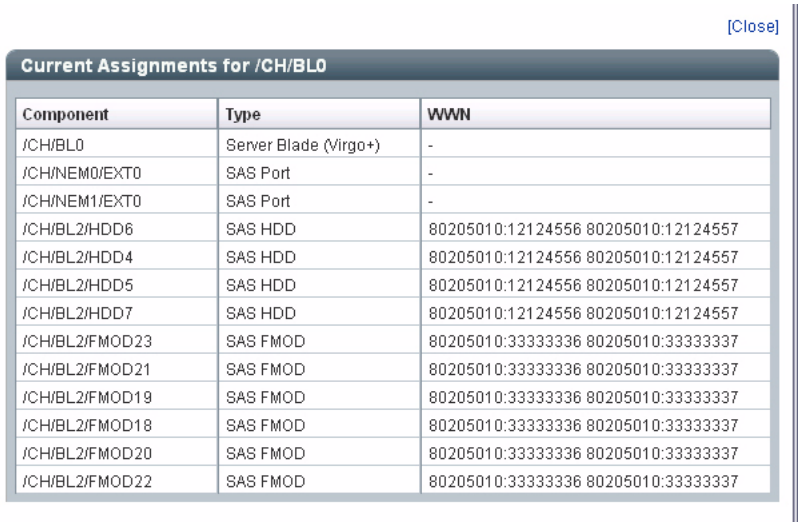
   b. **Scroll down to the Current Assignments table.**

      All of the storage resources that are currently assigned to the selected CPU blade server appear in the Current Assignments table.



3. **To view, at the same time, the Current Assignments table for the selected CPU blade server and the resource allocations for the other chassis CPU blade servers, click Detach Table.**

   The detached Current Assignments table appears in a separate dialog box.



Related Information

- "Modify Existing Blade Group Allocations (Web)" on page 254
- "Important SAS Zoning Allocations Considerations" on page 236
- "Manually Create SAS-2 Zoning Allocations (CLI)" on page 249
- *Sun Blade 6000 Modular System Documentation*

▼ Modify Existing Blade Group Allocations (Web)

Before You Begin

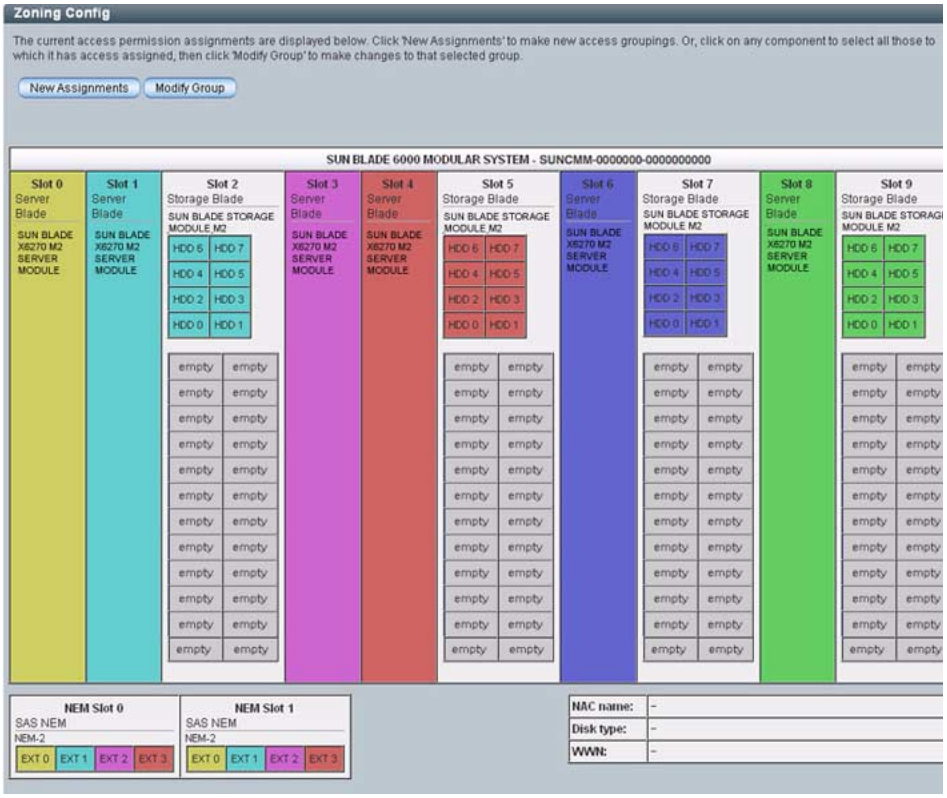
- Ensure that your chassis hardware configuration meets the requirements described in "Chassis Hardware Requirements" on page 237.
- Admin (a) role privileges are required in Oracle ILOM to modify any Sun Blade Zone Manager properties.
- The Sun Blade Zone Manager must be enabled in Oracle ILOM.

1. **To access the Sun Blade Zone Manager, click System Management > SAS Zoning.**

   The SAS Zoning page appears.

2. **In the Sun Blade Zone Manager section, click Detailed Setup.**

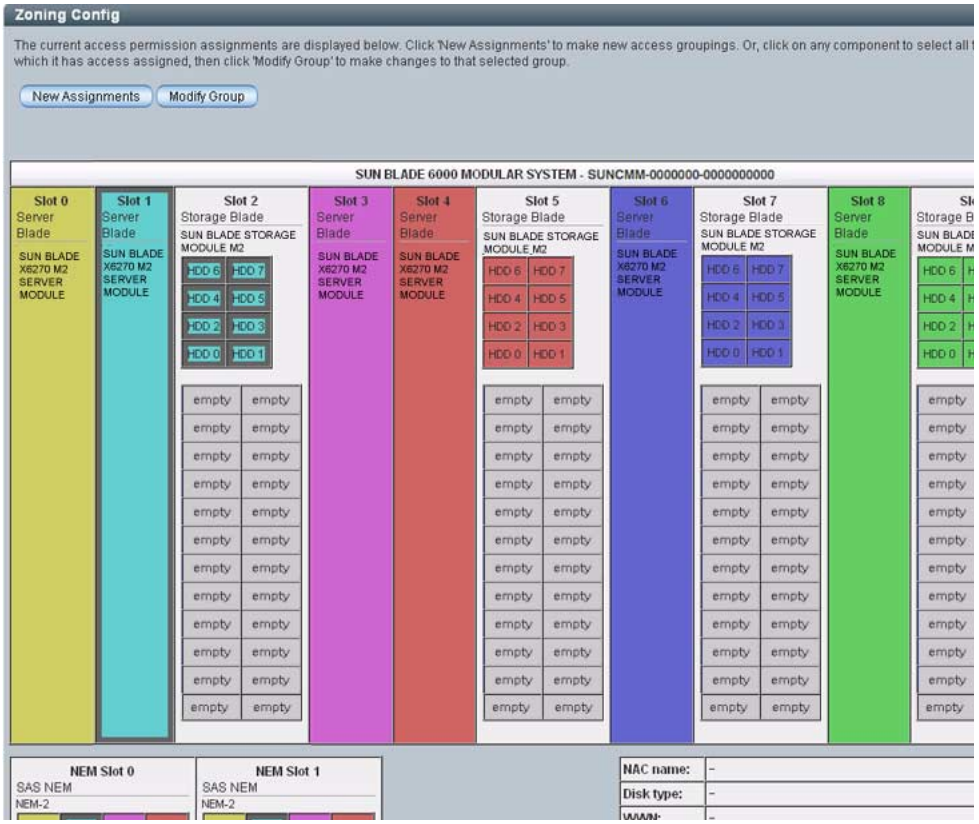
   The Zoning Config dialog appears, displaying the existing storage allocations in color-coded groups.



Note – Any HDD slots that do not have a storage device installed are labeled "empty." Empty HDD slots are not assigned to CPU blade servers.

3. **To modify the storage allocations for a blade storage group, select a blade that is part of the group.**

   The Sun Blade Zone Manager highlights the storage assigned to the blade storage group in the Zoning Config dialog.



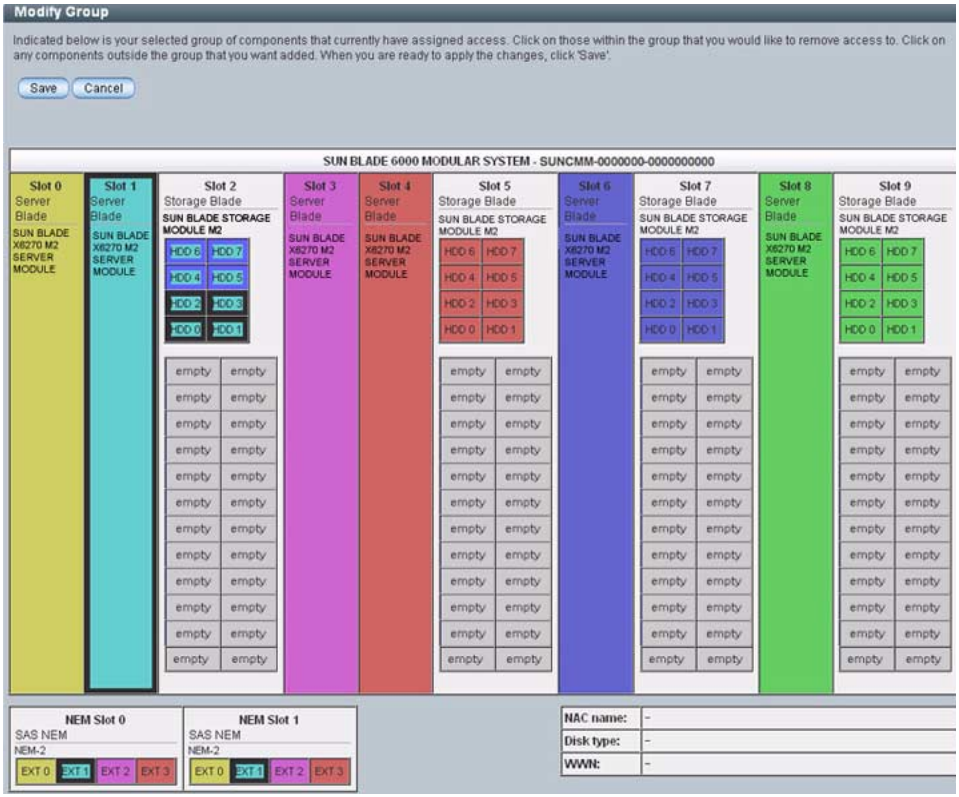
4. **To modify the storage resources assigned to a selected blade storage group, click Modify Group.**

   The Sun Blade Zone Manager highlights the selected blade storage group (which includes the storage resources currently assigned to the CPU blade server).

5. **Perform one or more of the following storage modifications to the selected group:**

   - To remove storage resources allocated to a selected blade storage group, click on the resources that you want to remove.

Example:
The following illustration depicts HDD 4-7 as selected resources to be removed from the CPU blade server in slot 1.



- To assign additional storage resources to a blade storage group, click on any storage resources outside the color-coded group that you want to add.

6. **To apply the allocation modifications made to the selected blade storage group, click Save.**

7. **Back up the saved the recently modified resource allocations.**

Related Information

- "Important SAS Zoning Allocations Considerations" on page 236
- "Backing Up and Recovering SAS-2 Zoning Assignments" on page 237
- "View and Modify Existing Storage Allocations (CLI)" on page 257
- *Sun Blade 6000 Modular System Documentation*

▼ View and Modify Existing Storage Allocations (CLI)

Before You Begin

- Ensure that your chassis hardware configuration meets the requirements in "Chassis Hardware Requirements" on page 237.
- Admin (a) role privileges in Oracle ILOM are required to view and modify the Sun Blade Zone Manager properties.
- The Sun Blade Zone Manager must be enabled in Oracle ILOM.

1. **Access the Sun Blade Zone Manager from the CLI.**

   See "Access and Enable Sun Blade Zone Manager" on page 238.

2. **To view storage resources allocated to a CPU blade server, perform one of the following.**

   - To view the storage allocations for a CPU blade server, use the `show` command followed by the `/STORAGE/sas_zoning/BL`*n* target. For example:

```
-> show /STORAGE/sas_zoning/BL0

   Targets:
      0      (/CH/BL2/HDD0)
      1      (/CH/BL2/HDD1)
```

     In this example, the HDD0 and HDD1, which are currently installed in the storage blade server in chassis slot 2, are allocated to the CPU blade server in chassis slot 0.

   - To view where a storage blade resource is allocated, use the `show` command followed by `/STORAGE/BL`*n*`/HDD`*n* target. For example:

```
-> show /STORAGE/BL2/HDD0

   Targets:
      0      (/CH/BL0)

-> show /STORAGE/BL2/HDD1

   Targets:
      0      (/CH/BL0)
```

     In this example, the resources HDD0 and HDD1, which are installed in the storage blade server in chassis slot 2, are assigned to the CPU blade server in chassis slot 0.

3. **To modify the storage allocations, perform one of the following methods:**

   Method 1: Add or unassign storage resources per CPU blade server.

   - To assign a storage resource to a CPU blade server, type:

     -> **cd /STORAGE/sas_zoning/BL***n*
     -> **set add_storage_access=***path_to_storage_device*

     Where BL*n* is the CPU blade server chassis slot location, and *path_to_storage_device* is the path to the storage blade resource.

   - To unassign a storage resource from a CPU blade server, type:

     -> **cd /STORAGE/sas_zoning/BL***n*
     -> **set remove_storage_access=***path_to_storage_device*

     Where BL*n* is the CPU blade server chassis slot location, and *path_to_storage_device* is the path to the resource on the storage blade server. For example, `/CH/BL1/HDD0`.

   Method 2: Add or unassign server blade access to storage device.

   - To assign a CPU blade server to a storage resource, type:

     -> **cd /STORAGE/sas_zoning/BL***n***/HDD***n*

     -> **set add_host_access=***path_to_blade_server*

   - To unassign a host server blade access to a storage device, type:

     -> **cd /STORAGE/sas_zoning/BL***n***/HDD***n*

     -> **set remove_host_access=***path_to_blade_server*

   Where BL*n* is the storage blade server chassis slot location, HDD*n* is the storage resource slot location, and *path_to_blade_server* is the chassis slot location for the CPU blade server that you want the resource assigned or unassigned. For example, `/CH/BL0`.

Note – You can also add or unassign multiple storage devices in a single command line. To do so, specify the full path to the resource and separate each resource with a comma (no space). For example:
-> **set add_storage_access=/CH/BL1/HDD0,/CH/BL1/HDD1**

---

4. **Back up the blade storage group assignment.**

Related Information

- "Important SAS Zoning Allocations Considerations" on page 236
- "Backing Up and Recovering SAS-2 Zoning Assignments" on page 237
- "Manually Create SAS-2 Zoning Allocations (CLI)" on page 249
- *Sun Blade 6000 Modular System Documentation*

Resetting Sun Blade Zone Manager Allocations to Factory Defaults

To erase all saved Sun Blade Zone Manager chassis storage allocations and to start the Sun Blade Zone Manager from factory defaults, perform one of the following procedures.

- "Reset Zoning Allocations to Factory Defaults (Web)" on page 259
- "Reset Zoning Allocations to Factory Defaults (CLI)" on page 259

▼ Reset Zoning Allocations to Factory Defaults (Web)

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify Sun Blade Zone Manager properties.

Caution – Use this procedure only if you want to erase all currently saved SAS zoning allocations in Oracle ILOM.

1. **To access the Sun Blade Zone Manager page in the CMM web interface, click System Management > SAS Zoning.**

   If the Sun Blade Manager state is enabled, a Reset All button appears in the Zoning Reset section of the Sun Blade Zone Manager page.

2. **To erase all saved resource allocations and reset the Sun Blade Zone Manager to factory defaults, click Reset All.**

▼ Reset Zoning Allocations to Factory Defaults (CLI)

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify Sun Blade Zone Manager properties.

Caution – Use this procedure only if you want to erase all currently saved SAS zoning allocations in Oracle ILOM.

1. **Navigate to** `/STORAGE/sas_zoning` **in the CMM CLI by using the following command:**

   ```
   -> cd /STORAGE/sas_zoning
   ```

2. **To erase all saved resource allocations and reset the Sun Blade Zone Manager to factory defaults, type:**

   ```
   -> set reset_access_action=true
   ```

   If the Zone Manager is disabled, you will get the following warning:

   ```
   set: The CMM is not the SAS Zone Manager
   ```

   If you receive this message, enable Zone Manager and re-issue the reset command. For details, see "Access and Enable Sun Blade Zone Manager" on page 238.

Resetting the Zoning Password to Factory Default for Third-Party In-Band Management

If you are managing storage allocations for chassis-level storage devices using a third-party in-band zone management application and you need to reset the zoning management password to the factory default, perform one of the following procedures.

- "Reset the Zoning Password (Web)" on page 260
- "Reset the Zoning Password (CLI)" on page 261

▼ Reset the Zoning Password (Web)

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify Sun Blade Zone Manager properties.

Caution – Use this procedure only if you are not using Oracle ILOM Zone Manager, and you are using a third-party in-band management application to manage the chassis storage allocations.

1. **To verify that the Sun Blade Zone Manager state is disabled in the CMM web interface, click System Management > SAS Zoning.**

   The Sun Blade Zone Manager page appears.

   If the Sun Blade Zone Manager is disabled, an option for resetting the password appears in the In-band Zoning Manager section.

2. **To reset the zoning password to the default value (all zeros), click Reset.**

▼ Reset the Zoning Password (CLI)

Before You Begin

- Admin (a) role privileges are required in Oracle ILOM to modify Sun Blade Zone Manager properties.

Caution – Use this procedure only if you are not using Oracle ILOM Zone Manager, and you are using a third-party in-band management application to manage the chassis storage allocations.

1. **Navigate to** `/STORAGE/sas_zoning` **using the following command:**

   -> **`cd /STORAGE/sas_zoning`**

2. **To reset the current zoning password, type:**

   -> **`set reset_password_action=true`**

   The password is set to the default (all zeros).

Index